JP00/5439

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

22/2

4

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年 ８月１２日

出 願 番 号
Application Number: 平成１１年特許願第２２８１５４号

出 願 人
Applicant (s): 松下電器産業株式会社

09/807295

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

２０００年 ８月２５日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号 出証特２０００－３０６８１６２

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社

【書類名】　特許願

【整理番号】　2030714021

【提出日】　平成11年 8月12日

【あて先】　特許庁長官殿

【国際特許分類】　H04M 15/00

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地
松下電器産業株式会社内

【氏名】　中西　良明

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地
松下電器産業株式会社内

【氏名】　高山　久

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地
松下電器産業株式会社内

【氏名】　松瀬　哲朗

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100082692

【弁理士】

【氏名又は名称】　蔵合　正博

【電話番号】　03(3519)2611

【手数料の表示】

【予納台帳番号】　013549

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9004843

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　電子価値情報バックアップシステム及びこれに用いる装置

【特許請求の範囲】

【請求項１】　電子現金・電子チケット等の電子価値情報を管理する電子財布手段と、前記電子財布手段が管理する電子価値情報を保持する電子財布記憶手段と、前記電子財布手段が管理する電子価値情報を通信によって登録することを受け付けその登録証を発行する電子金庫手段と前記電子価値情報を保管する電子金庫保管手段を持ち、前記電子財布手段は前記電子金庫手段に対して前記登録証を提示することで前記電子金庫保管手段に登録された前記電子価値情報を取り出すことが出来ることを特徴とする電子価値情報バックアップシステム。

【請求項２】　登録証に電子価値情報の部分情報が含まれることを特徴とする請求項１記載の電子価値情報バックアップシステム。

【請求項３】　電子財布手段固有の暗号鍵と復号鍵を保持する鍵保管手段と、前記暗号鍵を用いた暗号化および前記復号鍵を用いた復号化を行なう暗号化手段を追加し、電子価値情報を前記暗号化手段によって暗号化したものを電子金庫手段へ登録することを特徴とする請求項１記載の電子価値情報バックアップシステム。

【請求項４】　請求項３に鍵管理手段と前記鍵管理手段の記憶領域である鍵管理記憶手段を追加し、前記鍵管理手段に前記鍵保管手段に保持された復号鍵を暗号化手段が登録することによって、前記鍵保管手段の破損や紛失などの原因によって前記復号鍵が消失した時に前記暗号化手段が前記鍵管理手段から前記復号鍵を復元することを可能とすることを特徴とする請求項３記載の電子価値情報バックアップシステム。

【請求項５】　請求項３の鍵保管手段上に請求項３の暗号化手段が暗号鍵と復号鍵のペアを生成することを特徴とする請求項３記載の電子価値情報バックアップシステム。

【請求項６】　鍵管理手段が暗号鍵と復号鍵のペアを生成し、鍵保管手段に前記鍵ペアを配布することを特徴とする請求項４記載の電子価値情報バックアップシステム。

【請求項７】　鍵管理手段に復号鍵を２つに分割した一方の部分鍵を登録し、他方の部分鍵を暗号化された電子価値情報と組として電子金庫手段に登録することを特徴とする請求項４記載の電子価値情報バックアップシステム。

【請求項８】　請求項７での部分鍵として、暗号鍵と復号鍵を数学的に生成するための元となった情報を２つに分割して一方を鍵管理手段に登録する部分鍵、他方を電子金庫手段に登録する部分鍵とすることを特徴とする請求項７記載の電子価値情報バックアップシステム。

【請求項９】　電子財布手段から電子金庫手段に電子価値情報を登録し、前記電子金庫手段から送られた登録証に対する検証が成功した場合、登録済みの前記電子価値情報を電子財布手段から削除して対応する登録証のみを保管することを特徴とする請求項１記載の電子価値情報バックアップシステム。

【請求項１０】　暗号化手段が扱う暗号化方式を共通鍵方式として、暗号鍵と復号鍵に同じ鍵を用いることを特徴とする請求項３記載の電子価値情報バックアップシステム。

【請求項１１】　暗号化手段が扱う暗号化方式を公開鍵方式として、暗号鍵と復号鍵を非対称鍵とすることを特徴とする請求項３記載の電子価値情報バックアップシステム。

【請求項１２】　鍵保管手段の所有者固有の情報を鍵管理手段に復号鍵と関連付けて所有者認証情報として登録することと、前記所有者固有の情報を鍵管理手段に提示して認証が成功した場合に前記復号鍵を前記鍵保管手段に復元することを特徴とする請求項４記載の電子価値情報バックアップシステム。

【請求項１３】　所有者認証情報として鍵保管手段とは独立したＩＣカードに蓄積されたカード所有者を特定するための情報を用いることを特徴とする請求項１２記載の電子価値情報バックアップシステム。

【請求項１４】　所有者認証情報として所有者の生体特徴情報を用いることを特徴とする請求項１２記載の電子価値情報バックアップシステム。

【請求項１５】　鍵管理手段に対する所有者の正当性認証が成功した場合に、前記鍵管理手段が電子金庫手段と通信を行ない暗号化された電子価値情報を取得し、前記暗号化された電子価値情報の復号化を行なった電子価値情報を前記電子

財布記憶手段上に復元することを特徴とする請求項１２記載の電子価値情報バックアップ装置。

【請求項１６】　鍵管理手段に対して所有者の正当性認証が成功した場合に、前記鍵管理手段が電子金庫手段と通信を行ない暗号化された電子価値情報を取得し、前記暗号化された電子価値情報の復号化を行なった電子価値情報を新しく生成した暗号鍵を用いて暗号化し、前記の新しい暗号鍵で暗号化された前記電子価値情報を電子金庫上の古い暗号鍵で暗号化された前記電子価値情報と置き換え、前記鍵管理手段が新しい暗号鍵と復号鍵を鍵保管手段に配布することを特徴とする請求項１２記載の電子価値情報バックアップシステム。

【請求項１７】　鍵管理手段に対して所有者の正当性認証が成功した場合に、前記鍵管理手段が電子金庫手段と通信を行ない暗号化された電子価値情報を取得し、前記暗号化された電子価値情報の復号化を行なった電子価値情報を新しく生成した暗号鍵を用いて暗号化し、前記の新しい暗号鍵で暗号化された前記電子価値情報を電子財布手段上に復元し、前記鍵管理手段が新しい暗号鍵と復号鍵を鍵保管手段に配布することを特徴とする請求項１２記載の電子価値情報バックアップシステム。

【請求項１８】　電子財布手段が保管する電子価値情報に対して前記電子財布手段上のバックアップ条件情報と照合を行ない、条件に合致する電子価値情報を自動的に電子金庫手段に登録し登録証を受けとることを特徴とする請求項１記載の電子価値情報バックアップシステム。

【請求項１９】　バックアップ条件情報をユーザが変更できるようにすることを特徴とする請求項１８記載の電子価値情報バックアップシステム。

【請求項２０】　バックアップ条件情報として、電子価値情報の種類を用いることを特徴とする請求項１８記載の電子価値情報バックアップシステム。

【請求項２１】　バックアップ条件情報として、電子価値情報のサイズを用いることを特徴とする請求項１８記載の電子価値情報バックアップシステム。

【請求項２２】　バックアップ条件情報として、電子価値情報のサイズと電子財布記憶手段の空きメモリ容量を用いることを特徴とする請求項１８記載の電子価値情報バックアップシステム。

【請求項２３】　バックアップ条件情報として、電子価値情報の有効期限を用いることを特徴とする請求項１８記載の電子価値情報バックアップシステム。

【請求項２４】　バックアップ条件情報として、電子価値情報の保持開始時間を用いることを特徴とする請求項１８記載の電子価値情報バックアップシステム。

【請求項２５】　電子財布手段が登録証を提示して前記電子価値情報を前記電子財布手段上に復元する時、復元に十分な容量が電子財布上に残っていない場合、容量不足をユーザに対して提示し復元作業を中断することを特徴とする請求項１記載の電子価値情報バックアップシステム。

【請求項２６】　電子財布手段が登録証を提示して前記電子価値情報を前記電子財布手段上に復元する時または新規の電子価値情報を登録する時、復元や新規登録に十分な容量が電子財布記憶手段上に残っていない場合、電子財布手段上のバックアップ条件情報に基づいて現在保持されている電子価値情報を自動的に電子金庫手段に登録し登録証と置き換え、電子金庫上の電子価値情報を復元するための領域を空けることによって復元作業を継続することを特徴とする請求項１記載の電子価値情報バックアップシステム。

【請求項２７】　電子財布手段が電子価値情報の登録証を提示して前記電子価値情報を前記電子財布手段上に復元する時または新規の電子価値情報を登録する時、復元や新規登録に十分な容量が電子財布記憶手段上に残っていない場合、処理の中断および処理継続の方法を提示して選択させることで、復元作業の中断もしくは継続することを特徴とする請求項２６記載の電子価値情報バックアップシステム。

【請求項２８】　電子価値情報と登録証を保管する電子財布記憶手段を備え、電子金庫手段に対して通信を行うことを特徴とする電子財布手段。

【請求項２９】　登録証に電子価値情報の部分情報を含む事を特徴とする請求項２８記載の電子財布手段。

【請求項３０】　電子価値情報と登録証を保管する電子財布記憶手段と、電子価値情報を暗号化する暗号鍵と、暗号化された電子情報を復号化する復号鍵とを有する暗号化手段を備え、電子金庫手段に対して通信を行うことを特徴とする電

子財布手段。

【請求項３１】　請求項３０の復号鍵を２つに分割した部分鍵の一方を電子価値情報と組にして電子金庫手段に登録することを特徴とする請求項３０記載の電子財布手段。

【請求項３２】　請求項３１の部分鍵を、暗号鍵と復号鍵を数学的に生成する元となった情報を２つに分割した一方とすることを特徴とする請求項３１記載の電子財布手段。

【請求項３３】　前記電子金庫手段から送られた登録証が、バックアップする電子価値情報に対応する登録証であることを検証する登録証検証手段を備え、前記電子金庫手段から登録証を取得した際、前記登録証が前記バックアップする電子価値情報に対応する登録証であることが検証された場合に、前記登録証に対応する電子価値情報を電子財布記憶手段上から削除することを特徴とする請求項２８記載の電子財布手段。

【請求項３４】　設定されたバックアップ条件情報との照合を行ない、条件に合致する電子価値情報を自動的に電子金庫手段に登録して登録証を取得することを特徴とする請求項２８記載の電子財布手段。

【請求項３５】　電子価値情報の復元時または新規登録時に電子財布記憶手段上に十分な記憶容量が残っていない場合、容量不足をユーザに対して提示し復元作業を中断することを特徴とする請求項２８記載の電子財布手段。

【請求項３６】　電子価値情報の復元時または新規登録時に電子財布記憶手段上に十分な記憶容量が残っていない場合、自動的にバックアップ条件情報に基づいて電子価値情報のバックアップを行って記憶容量を確保することを特徴とする請求項２８記載の電子財布手段。

【請求項３７】　電子価値情報の復元時または新規登録時に電子財布記憶手段上に十分な記憶容量が残っていない場合、容量不足を提示して復元作業を中断するか自動的にバックアップ条件情報に基づいてバックアップを行なって記憶容量を確保するかをユーザに選択させることを特徴とする請求項２８記載の電子財布手段。

【請求項３８】　電子価値情報を保管する電子金庫記憶手段を備え、電子価値

情報から登録証を生成することと、登録証に対応する電子価値情報を電子金庫記憶手段から引き出すことを特徴とする電子金庫手段。

【請求項３９】　登録証に電子価値情報の部分情報が含まれる事を特徴とする請求項３８記載の電子金庫手段。

【請求項４０】　暗号化された電子価値情報の登録を受けて登録証を生成し、登録証の提示を受けて暗号化された電子価値情報を返すことを特徴とする請求項３８記載の電子金庫手段。

【請求項４１】　復号鍵を２つに分割した一方の部分鍵と暗号化した電子価値情報の登録を受けて登録証を生成し、登録証の提示を受けて暗号化された電子価値情報と部分鍵を返す事を特徴とする請求項４０記載の電子金庫手段。

【請求項４２】　請求項４１の部分鍵を、暗号鍵と復号鍵を数学的に生成する元となった情報を２つに分割した一方とすることを特徴とする請求項４１記載の電子金庫手段。

【請求項４３】　登録要求を受けた鍵を保管する鍵管理記憶手段を備える事を特徴とする鍵管理手段。

【請求項４４】　登録要求を受けた鍵を認証情報と組にして保管する鍵管理記憶手段を備え、認証情報が一致する場合のみ前記鍵管理記憶手段上に登録された鍵を引き出す事を可能とする事を特徴とする鍵管理手段。

【請求項４５】　暗号鍵と復号鍵の鍵ペアを生成して鍵管理記憶手段上に保管するとともに暗号化手段に対して配布する事を特徴とする鍵管理手段。

【請求項４６】　電子金庫手段と通信して、電子金庫手段上の暗号化された電子価値情報を鍵管理記憶手段上の復号鍵を用いて復号し、新しく暗号鍵と復号鍵の鍵ペアを生成し、新しい暗号鍵を用いて前記電子価値情報を暗号化した電子価値情報を古い暗号化された電子価値情報との置き換えることを電子金庫手段に対して要求し、新しい鍵ペアを暗号化手段に配布することを特徴とする鍵管理手段。

【請求項４７】　電子金庫手段と通信して、電子金庫手段上の暗号化された電子価値情報を鍵管理記憶手段上の復号鍵を用いて復号し、前記電子価値情報を電子財布手段に送ることを特徴とする鍵管理手段。

【請求項４８】　鍵管理手段と通信して所有者認証に基づいて復号鍵の登録と取得を行なうことを特徴とする暗号化手段。

【請求項４９】　電子金庫手段と通信して登録証と対応する一方の分割鍵を取得し、鍵管理手段と通信して所有者認証に基づいて他方の分割鍵を取得し、２つの分割鍵を用いて復号鍵を復元することを特徴とする暗号化手段。

【請求項５０】　請求項１から請求項２７および請求項２８から請求項３７に記載の電子財布手段の制御プログラムを、電子計算機が読み取り可能な形式で記録した制御プログラム記録媒体。

【請求項５１】　請求項１から請求項２７および請求項３７から請求項４２に記載の電子金庫手段の制御プログラムを、電子計算機が読み取り可能な形式で記録した制御プログラム記録媒体。

【請求項５２】　請求項３から請求項２７および請求項４３から請求項４７に記載の鍵管理手段の制御プログラムを、電子計算機が読み取り可能な形式で記録した制御プログラム記録媒体。

【請求項５３】　請求項２から請求項２７および請求項４８から請求項４９に記載の暗号化手段の制御プログラムを、電子計算機が読み取り可能な形式で記録した制御プログラム記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明はコンピュータと情報通信を用いたバックアップシステム、特に電子マネーや電子チケットといった電子価値情報のバックアップと復元を行なう電子価値情報システムに関するものである。

【０００２】

【従来の技術】

電子現金や電子チケットなどの金銭もしくは金銭的価値のある情報を、電子的な形式で表現し利用する技術が一般的となってきている。電子現金や電子チケットなどの電子的に表現された価値情報を、以下、電子価値情報とする。

【０００３】

電子価値情報の実現方法の一つとして、遠隔地のサーバ上で電子価値情報を置き、その所有者は認証情報のみを持ち、利用時にサーバと通信するようにする方法がある。前記の方法では、認証の安全性を確保する事によって安全な取り引きを実現できるが、ネットワークに接続できる状態でなければ電子価値情報を使用できないという問題や、ネットワークへの問い合わせが使用の度に発生するため、高速な反応を要求する状況には適用しにくいという問題がある。

【０００４】

そのため、ネットワークと独立した状態でも電子価値情報を利用することが出来るように、電子価値所有者の持つICカード、携帯電話、携帯端末などのデバイス上に電子価値情報そのものを保持するようにする技術も存在する。ただしこの場合、デバイスの破損や紛失によって電子価値情報が消失してしまう危険性を持っている。

【０００５】

上記の電子価値情報を含む電子情報の破壊という問題からの回復を実現するため、従来いくつかの技術が考案されている。以下にその例を示す。

【０００６】

第一の従来技術として、特開平１０－１３３９２５号公報に示される技術では、暗号化したメールを用いることで、ファイヤーウォール内から外のバックアップサーバに対してデータのバックアップを行う。ただしこの技術では、鍵の紛失や破損時に暗号化したデータからの復元方法についてを考慮していない。

【０００７】

第二の従来技術として、米国特許５，７７８，３９５に示される技術では、ネットワークに繋がったノード(コンピュータ)のファイルを別のノード上のサーバに圧縮や暗号化を行ってバックアップする。ただしこの技術でも、第一の従来技術と同様に鍵の紛失や破損時のことを考慮していない。

【０００８】

【発明が解決しようとする課題】

しかしながら、上述の従来技術は、暗号によって秘匿した状態で電子情報のバックアップと復元を行うものであった。しかし、従来技術では、暗号に用いた鍵

情報が消失した場合に暗号化されたバックアップ情報を復元することについて考慮されていないため、デバイスの破壊などに対処できないという問題がある。また、暗号の復号に用いる鍵をバックアップする場合、鍵のバックアップ管理の信頼性によらず、不正行為を排除しなければならない。

【０００９】

本発明は、上記のような問題に鑑みてなされたもので、通信を介してサーバ上に電子価値情報を安全にバックアップすることと、バックアップと復元の際に不正行為が行われないことと、鍵情報消失の緊急時の電子価値情報のバックアップからの復元を可能とする手段を提供することを目的とする。

【００１０】

【課題を解決するための手段】

上記課題を解決するために、本発明は第１にローカルの電子価値情報を暗号化してサーバ上にバックアップする。これにより、電子価値情報をサーバに隠蔽した状態でバックアップすることと、ローカルの電子価値情報が破損した場合にも電子価値情報を復元することが可能になる。

【００１１】

また、第２に暗号化した電子価値情報の復号鍵を電子価値情報のバックアップ先のサーバとは別のサーバにバックアップする。これにより、ローカルの復号鍵が破損した場合にも復号鍵を復元する事によって暗号化した電子価値情報を復元する事が可能になる。

【００１２】

また、第３に復号鍵を分割してそれぞれを別々にバックアップする。これにより、復号鍵の全体を知られる事なく、ローカルに復号鍵を復元することが可能になる。

【００１３】

また、第４に復号鍵をバックアップしたサーバに、暗号化した電子価値情報を復号させて電子価値情報をローカルに復元する。これにより、ローカルデバイスが壊滅的に破損または紛失した場合にも、電子価値情報を復元する事が可能になる。

【００１４】

また、第５に復号鍵をバックアップしたサーバに、暗号化した電子価値情報を復号させ、新しい暗号化を行なわせて登録しなおし、新しい鍵情報をローカル環境に再配布させる。これにより、ローカル環境の鍵情報のみが破損または紛失した場合にも、ローカル環境に与える影響を小さく抑えた上でバックアップした電子価値情報を復元できる環境を再構築することが可能となる。

【００１５】

このような各種態様を有する発明として、本発明の請求項１に記載の発明は、電子価値情報バックアップシステムとして、電子現金・電子チケット等の電子価値情報を管理する電子財布手段と、前記電子財布手段が管理する電子価値情報を保持する電子財布記憶手段と、前記電子財布手段が管理する電子価値情報を通信によって登録することを受け付けその登録証を発行する電子金庫手段と前記電子価値情報を保管する電子金庫保管手段を持ち、前記電子財布手段は前記電子金庫手段に対して前記登録証を提示することで前記電子金庫保管手段に登録された前記電子価値情報を取り出すことが出来るようにしたものである。

【００１６】

本発明の請求項２に記載の発明は、請求項１記載の電子価値情報バックアップシステムにおいて、登録証に電子価値情報の部分情報が含まれるようにしたものである。

【００１７】

本発明の請求項３に記載の発明は、請求項１記載の電子価値情報バックアップシステムにおいて、電子財布手段固有の暗号鍵と復号鍵を保持する鍵保管手段と、前記暗号鍵を用いた暗号化および前記復号鍵を用いた復号化を行なう暗号化手段を追加し、電子価値情報を前記暗号化手段によって暗号化したものを電子金庫手段へ登録するようにしたものである。

【００１８】

本発明の請求項４に記載の発明は、請求項３記載の電子価値情報バックアップシステムにおいて、請求項３に鍵管理手段と前記鍵管理手段の記憶領域である鍵管理記憶手段を追加し、前記鍵管理手段に前記鍵保管手段に保持された復号鍵を

暗号化手段が登録することによって、前記鍵保管手段の破損や紛失などの原因によって前記復号鍵が消失した時に前記暗号化手段が前記鍵管理手段から前記復号鍵を復元することを可能としたものである。

【００１９】

本発明の請求項５に記載の発明は、請求項３記載の電子価値情報バックアップシステムにおいて、請求項３の鍵保管手段上に請求項３の暗号化手段が暗号鍵と復号鍵のペアを生成するようにしたものである。

【００２０】

本発明の請求項６に記載の発明は、請求項４記載の電子価値情報バックアップシステムにおいて、鍵管理手段が暗号鍵と復号鍵のペアを生成し、鍵保管手段に前記鍵ペアを配布するようにしたものである。

【００２１】

本発明の請求項７に記載の発明は、請求項４記載の電子価値情報バックアップシステムにおいて、鍵管理手段に復号鍵を２つに分割した一方の部分鍵を登録し、他方の部分鍵を暗号化された電子価値情報と組として電子金庫手段に登録するようにしたものである。

【００２２】

本発明の請求項８に記載の発明は、請求項７記載の電子価値情報バックアップシステムにおいて、請求項７での部分鍵として、暗号鍵と復号鍵を数学的に生成するための元となった情報を２つに分割して一方を鍵管理手段に登録する部分鍵、他方を電子金庫手段に登録する部分鍵とするようにしたものである。

【００２３】

本発明の請求項９に記載の発明は、請求項１記載の電子価値情報バックアップシステムにおいて、電子財布手段から電子金庫手段に電子価値情報を登録し、前記電子金庫手段から送られた登録証に対する検証が成功した場合、登録済みの前記電子価値情報を電子財布手段から削除して対応する登録証のみを保管するようにしたものである。

【００２４】

本発明の請求項１０に記載の発明は、請求項３記載の電子価値情報バックアッ

プシステムにおいて、暗号化手段が扱う暗号化方式を共通鍵方式として、暗号鍵と復号鍵に同じ鍵を用いるようにしたものである。

【００２５】

本発明の請求項１１に記載の発明は、請求項３記載の電子価値情報バックアップシステムにおいて、暗号化手段が扱う暗号化方式を公開鍵方式として、暗号鍵と復号鍵を非対称鍵とするようにしたものである。

【００２６】

本発明の請求項１２に記載の発明は、請求項４記載の電子価値情報バックアップシステムにおいて、鍵保管手段の所有者固有の情報を鍵管理手段に復号鍵と関連付けて所有者認証情報として登録することと、前記所有者固有の情報を鍵管理手段に提示して認証が成功した場合に前記復号鍵を前記鍵保管手段に復元するようにしたものである。

【００２７】

本発明の請求項１３に記載の発明は、請求項１０記載の電子価値情報バックアップシステムにおいて、所有者認証情報として鍵保管手段とは独立したＩＣカードに蓄積されたカード所有者を特定するための情報を用いるようにしたものである。

【００２８】

本発明の請求項１４に記載の発明は、請求項１２記載の電子価値情報バックアップシステムにおいて、所有者認証情報として所有者の生体特徴情報を用いるようにしたものである。

【００２９】

本発明の請求項１５に記載の発明は、請求項１２記載の電子価値情報バックアップシステムにおいて、鍵管理手段に対する所有者の正当性認証が成功した場合に、前記鍵管理手段が電子金庫手段と通信を行ない暗号化された電子価値情報を取得し、前記暗号化された電子価値情報の復号化を行なった電子価値情報を前記電子財布記憶手段上に復元するようにしたものである。

【００３０】

本発明の請求項１６に記載の発明は、請求項１２記載の電子価値情報バックア

ップシステムにおいて、鍵管理手段に対して所有者の正当性認証が成功した場合に、前記鍵管理手段が電子金庫手段と通信を行ない暗号化された電子価値情報を取得し、前記暗号化された電子価値情報の復号化を行なった電子価値情報を新しく生成した暗号鍵を用いて暗号化し、前記の新しい暗号鍵で暗号化された前記電子価値情報を電子金庫上の古い暗号鍵で暗号化された前記電子価値情報と置き換え、前記鍵管理手段が新しい暗号鍵と復号鍵を鍵保管手段に配布するようにしたものである。

【００３１】

本発明の請求項１７に記載の発明は、請求項１２記載の電子価値情報バックアップシステムにおいて、鍵管理手段に対して所有者の正当性認証が成功した場合に、前記鍵管理手段が電子金庫手段と通信を行ない暗号化された電子価値情報を取得し、前記暗号化された電子価値情報の復号化を行なった電子価値情報を新しく生成した暗号鍵を用いて暗号化し、前記の新しい暗号鍵で暗号化された前記電子価値情報を電子財布手段上に復元し、前記鍵管理手段が新しい暗号鍵と復号鍵を鍵保管手段に配布するようにしたものである。

【００３２】

本発明の請求項１８に記載の発明は、請求項１２記載の電子価値情報バックアップシステムにおいて、電子財布手段が保管する電子価値情報に対して前記電子財布手段上のバックアップ条件情報と照合を行ない、条件に合致する電子価値情報を自動的に電子金庫手段に登録し登録証を受けとるようにしたものである。

【００３３】

本発明の請求項１９に記載の発明は、請求項１８記載の電子価値情報バックアップシステムにおいて、バックアップ条件情報をユーザが変更できるようにしたものである。

【００３４】

本発明の請求項２０に記載の発明は、請求項１８記載の電子価値情報バックアップシステムにおいて、バックアップ条件情報として、電子価値情報の種類を用いるようにしたものである。

【００３５】

本発明の請求項２１に記載の発明は、請求項１８記載の電子価値情報バックアップシステムにおいて、バックアップ条件情報として、電子価値情報のサイズを用いるようにしたものである。

【００３６】

本発明の請求項２２に記載の発明は、請求項１８記載の電子価値情報バックアップシステムにおいて、バックアップ条件情報として、電子価値情報のサイズと電子財布記憶手段の空きメモリ容量を用いるようにしたものである。

【００３７】

本発明の請求項２３に記載の発明は、請求項１８記載の電子価値情報バックアップシステムにおいて、バックアップ条件情報として、電子価値情報の有効期限を用いるようにしたものである。

【００３８】

本発明の請求項２４に記載の発明は、請求項１８記載の電子価値情報バックアップシステムにおいて、バックアップ条件情報として、電子価値情報の保持開始時間を用いるようにしたものである。

【００３９】

本発明の請求項２５に記載の発明は、請求項１記載の電子価値情報バックアップシステムにおいて、電子財布手段が登録証を提示して前記電子価値情報を前記電子財布手段上に復元する時、復元に十分な容量が電子財布上に残っていない場合、容量不足をユーザに対して提示し復元作業を中断するようにしたものである。

【００４０】

本発明の請求項２６に記載の発明は、請求項１記載の電子価値情報バックアップシステムにおいて、電子財布手段が登録証を提示して前記電子価値情報を前記電子財布手段上に復元する時または新規の電子価値情報を登録する時、復元や新規登録に十分な容量が電子財布記憶手段上に残っていない場合、電子財布手段上のバックアップ条件情報に基づいて現在保持されている電子価値情報を自動的に電子金庫手段に登録し登録証と置き換え、電子金庫上の電子価値情報を復元するための領域を空けることによって復元作業を継続するようにしたものである。

【００４１】

本発明の請求項２７に記載の発明は、請求項２６記載の電子価値情報バックアップシステムにおいて、電子財布手段が電子価値情報の登録証を提示して前記電子価値情報を前記電子財布手段上に復元する時または新規の電子価値情報を登録する時、復元や新規登録に十分な容量が電子財布記憶手段上に残っていない場合、処理の中断および処理継続の方法を提示して選択させることで、復元作業の中断もしくは継続するようにしたものである。

【００４２】

本発明の請求項２８に記載の発明は、電子財布手段として、電子価値情報と登録証を保管する電子財布記憶手段を備え、電子金庫手段に対して通信を行うようにしたものである。

【００４３】

本発明の請求項２９に記載の発明は、請求項２８記載の電子財布手段において、登録証に電子価値情報の部分情報を含むようにしたものである。

【００４４】

本発明の請求項３０に記載の発明は、電子財布手段として、電子価値情報と登録証を保管する電子財布記憶手段と、電子価値情報を暗号化する暗号鍵と、暗号化された電子情報を復号化する復号鍵とを有する暗号化手段を備え、電子金庫手段に対して通信を行うようにしたものである。

【００４５】

本発明の請求項３１に記載の発明は、請求項３０記載の電子財布手段において、請求項３０の復号鍵を２つに分割した部分鍵の一方を電子価値情報と組にして電子金庫手段に登録するようにしたものである。

【００４６】

本発明の請求項３２に記載の発明は、請求項３１記載の電子財布手段において、請求項３１の部分鍵を、暗号鍵と復号鍵を数学的に生成する元となった情報を２つに分割した一方とするようにしたものである。

【００４７】

本発明の請求項３３に記載の発明は、請求項２８記載の電子財布手段において

、前記電子金庫手段から送られた登録証が、バックアップする電子価値情報に対応する登録証であることを検証する登録証検証手段を備え、前記電子金庫手段から登録証を取得した際、前記登録証が前記バックアップする電子価値情報に対応する登録証であることが検証された場合に、前記登録証に対応する電子価値情報を電子財布記憶手段上から削除するようにしたものである。

【００４８】

本発明の請求項３４に記載の発明は、請求項２８記載の電子財布手段において、設定されたバックアップ条件情報との照合を行ない、条件に合致する電子価値情報を自動的に電子金庫手段に登録して登録証を取得するようにしたものである。

【００４９】

本発明の請求項３５に記載の発明は、請求項２８記載の電子財布手段において、電子価値情報の復元時または新規登録時に電子財布記憶手段上に十分な記憶容量が残っていない場合、容量不足をユーザに対して提示し復元作業を中断するようにしたものである。

【００５０】

本発明の請求項３６に記載の発明は、請求項２８記載の電子財布手段において、電子価値情報の復元時または新規登録時に電子財布記憶手段上に十分な記憶容量が残っていない場合、自動的にバックアップ条件情報に基づいて電子価値情報のバックアップを行って記憶容量を確保するようにしたものである。

【００５１】

本発明の請求項３７に記載の発明は、請求項２８記載の電子財布手段において、電子価値情報の復元時または新規登録時に電子財布記憶手段上に十分な記憶容量が残っていない場合、容量不足を提示して復元作業を中断するか自動的にバックアップ条件情報に基づいてバックアップを行なって記憶容量を確保するかをユーザに選択させるようにしたものである。

【００５２】

本発明の請求項３８に記載の発明は、電子金庫手段として、電子価値情報を保管する電子金庫記憶手段を備え、電子価値情報から登録証を生成することと、登

録証に対応する電子価値情報を電子金庫記憶手段から引き出すようにしたものである。

【００５３】

本発明の請求項３９に記載の発明は、請求項３８記載の電子金庫手段において、登録証に電子価値情報の部分情報が含まれるようにしたものである。

【００５４】

本発明の請求項４０に記載の発明は、請求項３８記載の電子金庫手段において、暗号化された電子価値情報の登録を受けて登録証を生成し、登録証の提示を受けて暗号化された電子価値情報を返すようにしたものである。

【００５５】

本発明の請求項４１に記載の発明は、請求項４０記載の電子金庫手段において、復号鍵を２つに分割した一方の部分鍵と暗号化した電子価値情報の登録を受けて登録証を生成し、登録証の提示を受けて暗号化された電子価値情報と部分鍵を返すようにしたものである。

【００５６】

本発明の請求項４２に記載の発明は、請求項４１記載の電子金庫手段において、請求項４１の部分鍵を、暗号鍵と復号鍵を数学的に生成する元となった情報を２つに分割した一方とするようにしたものである。

【００５７】

本発明の請求項４３に記載の発明は、鍵管理手段として、登録要求を受けた鍵を保管する鍵管理記憶手段を備えたものである。

【００５８】

本発明の請求項４４に記載の発明は、鍵管理手段として、登録要求を受けた鍵を認証情報と組にして保管する鍵管理記憶手段を備え、認証情報が一致する場合のみ前記鍵管理記憶手段上に登録された鍵を引き出すようにしたものである。

【００５９】

本発明の請求項４５に記載の発明は、鍵管理手段として、暗号鍵と復号鍵の鍵ペアを生成して鍵管理記憶手段上に保管するとともに暗号化手段に対して配布するようにしたものである。

【００６０】

本発明の請求項４６に記載の発明は、鍵管理手段として、電子金庫手段と通信して、電子金庫手段上の暗号化された電子価値情報を鍵管理記憶手段上の復号鍵を用いて復号し、新しく暗号鍵と復号鍵の鍵ペアを生成し、新しい暗号鍵を用いて前記電子価値情報を暗号化した電子価値情報を古い暗号化された電子価値情報との置き換えることを電子金庫手段に対して要求し、新しい鍵ペアを暗号化手段に配布するようにしたものである。

【００６１】

本発明の請求項４７に記載の発明は、鍵管理手段として、電子金庫手段と通信して、電子金庫手段上の暗号化された電子価値情報を鍵管理記憶手段上の復号鍵を用いて復号し、前記電子価値情報を電子財布手段に送るようにしたものである。

【００６２】

本発明の請求項４８に記載の発明は、暗号化手段として、鍵管理手段と通信して所有者認証に基づいて復号鍵の登録と取得を行なうことを特徴とする暗号化手段。

【００６３】

本発明の請求項４９に記載の発明は、暗号化手段として、電子金庫手段と通信して登録証と対応する一方の分割鍵を取得し、鍵管理手段と通信して所有者認証に基づいて他方の分割鍵を取得し、２つの分割鍵を用いて復号鍵を復元するようにしたものである。

【００６４】

本発明の請求項５０に記載の発明は、制御プログラム記録媒体として、請求項１から請求項２７および請求項２８から請求項３７に記載の電子財布手段の制御プログラムを、電子計算機が読み取り可能な形式で記録したことを特徴とするものである。

【００６５】

本発明の請求項５１に記載の発明は、制御プログラム記録媒体として、請求項１から請求項２７および請求項３７から請求項４２に記載の電子金庫手段の制御

プログラムを、電子計算機が読み取り可能な形式で記録したことを特徴とするものである。

【００６６】

本発明の請求項５２に記載の発明は、制御プログラム記録媒体として、請求項３から請求項２７および請求項４３から請求項４７に記載の鍵管理手段の制御プログラムを、電子計算機が読み取り可能な形式で記録したことを特徴とするものである。

【００６７】

本発明の請求項５３に記載の発明は、制御プログラム記録媒体として、請求項２から請求項２７および請求項４８から請求項４９に記載の暗号化手段の制御プログラムを、電子計算機が読み取り可能な形式で記録したことを特徴とするものである。

【００６８】

【発明の実施形態】

以下、図１から図１８を用いて本発明の実施の形態について説明する。なお、本発明はこれらの実施の形態に何等限定されるものではなく、その要旨を逸脱しない範囲に置いて種々なる態様で実施し得る。

【００６９】

（実施の形態１）

図１から３と図７を用いて、請求項１から請求項２と請求項９と請求項２８から請求項２９と請求項３３と請求項３８から請求項３９との実施の形態について述べる。

【００７０】

図１は、本実施の形態が示す電子価値情報バックアップシステムの一例を示した構成図である。本システムは基本的に有線または無線の通信路によって結ばれたコンピュータ装置と、それに接続された外部拡張機器およびそれらの上で動作するソフトウェアで構成されるものとする。ここでいうコンピュータ装置とは、ソフトウエアプログラムにしたがって動作するＣＰＵを備えた機器の総称を意味するものとする。

【００７１】

本実施の形態では、電子財布手段１０１および電子財布記憶手段１０２はＩＣカード１２１の中に構成される。端末１００はＩＣカードリーダを備えた携帯電話端末であり、ＩＣカード１２１内に構成された電子財布手段１０１と通信することが出来る。端末１００と電子金庫手段１０３は、無線によって通信を行なう。なお、端末１００は、ＩＣカードリーダを備えた、パーソナルコンピュータ、または、セットトップボックス、または、携帯型端末であっても良い。また、端末１００と電子金庫手段１０３の間の通信は、有線通信であってもよい。また、電子財布手段１０１と電子財布記憶手段１０２をＩＣカード中ではなく、端末１００上に内蔵する形で構成してもよい。

【００７２】

電子財布手段１０１はソフトウェアと前記ソフトウェア格納する記憶領域と前記ソフトウェアを解釈して実行するためのＯＳおよびＣＰＵによって実現される。また、電子財布手段１０１は電子財布記憶手段１０２の内容の参照と変更を行なうことができる。電子財布記憶手段１０２はＥＥＰＲＯＭなどの書き換え可能なメモリによって実現される。

【００７３】

電子価値情報とは電子現金や電子チケットなどを表す電子情報であり、登録証とは前記電子価値情報を電子金庫手段１０３に登録したさいに発行される前記電子価値情報の控えを表す電子情報である。図３に電子財布記憶手段１０２での電子価値情報と登録証の管理方法を示す。電子財布手段１０１は電子財布記憶手段１０２上にインデックス８５１を置く。前記インデックス８５１は、電子財布記憶手段１０２上に格納された情報に対するポインタと前記情報のサイズとポインタの先の情報の種別を表す記号の組をまとめたものである。これにより、電子財布手段１０１は次に示す機能を実現できる。

【００７４】

電子財布手段１０１は電子財布記憶手段１０２中のインデックス８５１を参照してポインタとサイズを取得し、取得したポインタとサイズを用いて電子価値情報または登録証を取り出すことができる。また、この電子財布手段１０１は電子

財布記憶手段１０２中のインデックス８５１を参照してすべてのポインタとサイズを取得し、それを用いて、すべての電子価値情報と登録証のタイトル情報を取得する。前記のポインタとサイズタイトルを用いて、全保管情報のリストを作成することができる。また、特定の条件に合致するポインタとサイズを取得することで、条件に合致する情報のリスト（例えば登録証のリストや有効期限完了まで残り一週間以内の情報のリストなど）を作成することもできる。

【００７５】

電子財布手段１０１は、電子財布記憶手段１０２中の空き領域に電子価値情報または登録証を書き込み、それに対応する種別とポインタとサイズの組のエントリをインデックス８５１に追加することで、電子財布記憶手段１０２に電子価値情報または登録証を保管することができる。またその逆に、インデックス８５１中に示されたポインタとサイズを参照して、前記ポインタとサイズが指す領域を消去し、前記ポインタとサイズに対応したエントリをインデックス８５１から削除することで、電子財布記憶手段１０２から電子価値情報または登録証を削除することができる。また、新規登録と削除を組み合わせることで、電子価値情報または登録証の情報を修正することができる。なお、上記の仕組み或いは機能はＩＣカード２０１上のオペレーティングシステム（ＯＳ）が持つ機能を用いて実現しても良い。

【００７６】

電子金庫手段１０３はワークステーションまたはパーソナルコンピュータなどのコンピュータ装置と、前記コンピュータシステム上で動作するソフトウェアから構成される。電子金庫手段１０３は電子金庫記憶手段１１０の内容の参照と変更を行なうことができる。電子金庫記憶手段１１０は電子金庫手段１０３が内容の参照と変更を行なうことができる記憶装置であり、ハードディスクなどで実現される。電子金庫記憶手段１１０上には前記コンピュータシステムのＯＳが管理するファイルシステムが構築されている。図２（ａ）に電子価値情報の一例として電子価値情報２０１を示す。電子金庫手段１０３が電子価値情報２０１の登録要求を受けた場合、図２（ｃ）に示す登録証３０１を電子価値情報２０１を用いて生成する。登録証３０１を生成する処理の流れを以下に説明する。

【００７７】

電子金庫手段１０３は設定に基づいて、電子価値情報２０１から図２（ｂ）に示すダイジェスト３０２を生成する。また、電子価値情報２０１を一方向性のハッシュ関数に通してＸ１という数を生成する。電子金庫手段１０３が持つカウンタを参照しＹ１という数を取得する。前記カウンタは参照の度に１ずつ昇順で増加し、上限に達すれば０に戻るものであるとする。これらダイジェスト３０２とハッシュ値Ｘ１とカウンタ値Ｙ１を組として登録証３０１とする。前記Ｘ１を生成するために用いたハッシュ関数として、ＭＤ５やＳＨＡ１などの分散性の高いものを用いることとする。なお、ダイジェスト３０２は空情報であってもよい。

【００７８】

図７に電子金庫記憶手段１１０での情報の保管方法を示す。電子金庫記憶手段１１０は、電子価値情報２０１をファイル８０１、登録証３０１をファイル８０２として保管する。登録証３０１の構成要素であるハッシュ値Ｘ１とカウンタ値Ｙ１とファイル８０１のパス情報とファイル８０２のパス情報を組として、インデックスファイル８５２の１つのエントリとして登録する。インデックスファイル８５２は１エントリ１行のＣＳＶファイルであり、各行はカウンタ値によって昇順にソートされている。端末１００から電子金庫手段１０３に登録証が提示された場合に、インデックスファイル８５２から登録証に対応する電子価値情報をカウンタ値の一致するエントリ群を検索し、その中からハッシュ値が一致するエントリ群にさらに絞り込み、登録証が完全に一致するエントリを抽出する。これにより登録証に対応する電子価値情報を高速に検索することが可能である。

【００７９】

ユーザが端末１００を操作して電子価値情報２０１をバックアップする手順を、以上に示した各手段を用いて示す。以下の手順での選択動作はすべてユーザによって行なわれれる。

(1-1) 端末１００が、電子財布手段１０１に電子価値情報リストを要求する。電子財布手段１０１は電子価値情報のリストを生成し、端末１００に送る。

(1-2) 端末１００が、電子価値情報リストから選択した電子価値情報２０１を電子財布手段１０１に要求する。電子財布手段１０１は電子価値情報２０１を電子

財布記憶手段１０２から取得し、端末１００に送る。

(1-3) 端末１００が、電子価値情報２０１の登録を電子金庫手段１０３に要求する。電子金庫手段１０３は電子価値情報２０１を電子金庫記憶手段１１０に保管すると同時に、電子価値情報２０１から登録証３０１を生成し、登録証３０１を端末１００に送る。

(1-4) 端末１００が、登録証３０１の保管を電子財布手段１０１に要求する。電子財布手段１０１は、電子価値情報２０１の内容と登録証３０１のダイジェスト３０２とを、電子価値情報２０１をハッシュ演算した値と登録証３０１のハッシュ値Ｘ１とを、それぞれ照合し、一致した場合に、登録証３０１を電子財布記憶手段１０２に保管し、完了通知を端末１００に送る。一致しなかった場合には、電子財布手段１０１は、電子価値情報２０１のバックアップを中止し、エラー通知を端末１００に送る。

【００８０】

なお、登録証３０１が正常に電子財布記憶手段１０２に保管された場合、電子財布記憶手段１０２上から電子価値情報２０１を削除してもよい。ＩＣカードのように記憶容量が少ないデバイスを用いる場合、これは記憶容量を効率的に利用する有効な手段である。

【００８１】

同様に、ユーザが端末１００を操作して電子財布記憶手段１０２に保管された登録証３０１に対応する電子価値情報２０１を電子財布記憶手段１０２上に復元する手順を次に示す。

(2-1) 端末１００が、電子財布手段１０１に登録証リストを要求する。電子財布手段１０１は登録証リストを生成し、端末１００に送る。

(2-2) 端末１００が、登録証リストから選択した登録証３０１を電子財布手段１０１に要求する。電子財布手段１０１は登録証３０１を電子財布記憶手段１０２から取得し、端末１００に送る。

(2-3) 端末１００が、電子金庫手段１０３に登録証３０１を提示し、対応する電子価値情報の取得を要求する。電子金庫手段１０３は登録証３０１を用いて電子価値情報２０１を検索して取得し、端末１００に送る。この時、電子金庫手段１

０３は、検索した電子価値情報の内容と登録証３０１とを照合し、不整合がたった場合には、電子価値情報２０１の復元処理を中止する。

(2-4) 端末１００が、電子価値情報２０１の登録を電子財布手段１０１に要求する。電子財布手段１０１は電子価値情報２０１を電子財布記憶手段１０２に保管し、完了通知を取得する。

【００８２】

以上に説明したシステムを用いることで、ユーザが持つ電子価値情報を電子金庫記憶手段上にバックアップすることと、バックアップした電子価値情報の概要を電子金庫手段に問い合わせることなく知ることと、必要に応じて電子価値情報を電子財布記憶手段上に復元することが可能となる。

【００８３】

【実施の形態２】

図４から６を用いて、請求項３と請求項５と請求項１０から１１と請求項３０と請求項４０の実施の形態について述べる。図４は本実施の形態における電子価値情報バックアップシステムの一例を示した構成図であり、本システムは実施の形態１（図１）で示されたシステムの端末１００を端末１１２に置き換え、電子金庫手段１０３を電子金庫手段１１３に置き換え、ＩＣカード１２１をＩＣカード１２２と置き換えたものである。ＩＣカード１２２はＩＣカード１２１に対して暗号化手段１０５と鍵保管手段１０４を追加し、電子財布手段１０１を電子財布手段１１１に変更したものである。

【００８４】

暗号化手段１０５は、ソフトウェアと前記ソフトウェアを格納する記憶領域と前記ソフトウェアを解釈して実行するためのＯＳおよびＣＰＵによって構成される。鍵保管手段１０４はＥＥＰＲＯＭなどの書き換え可能なメモリによって実現される。なお、暗号化手段１０５と電子財布手段１１１はＯＳとＣＰＵを共有してもよい。また、鍵保管手段１０４と電子財布記憶手段１０２はＥＥＰＲＯＭを共有してもよい。

【００８５】

鍵保管手段１０４は暗号鍵４０１と復号鍵４０２を保持する（図６）。本実施

の形態では、鍵保管手段１０４に保管された暗号鍵４０１と復号鍵４０２のペアは、暗号化手段１０５が生成する。暗号化手段１０５は公開鍵暗号方式を用いることとし、暗号鍵４０１を公開鍵、復号鍵４０２を秘密鍵とする。なお、暗号化手段１０５の暗号化方式として共有鍵暗号方式を用いてもよい。その場合、暗号鍵４０１と復号鍵４０２は同一の鍵となる。

【００８６】

暗号化手段１０５は、鍵保管手段１０４から暗号鍵４０１を取得し、電子価値情報２０１を入力として電子価値情報２０２を生成する。図５は登録電子価値情報２０３を示したものである。登録電子価値情報２０３は、ダイジェスト３０２と、電子価値情報２０１を暗号鍵４０１で暗号化した暗号化電子価値情報２０２と、ダイジェスト３０２と暗号化電子価値情報２０２をまとめて暗号鍵４０１で電子署名した署名３０３から構成される。暗号化手段１０５は、鍵保管手段１０４から復号鍵４０２を取得し、登録電子価値情報２０３を入力として電子価値情報２０１を再生する。暗号化手段１０５は復号鍵４０２を用いて署名３０３を検証して正当性が確認した後、暗号化電子価値情報２０２を復号化して電子価値情報２０１を生成する。

【００８７】

電子財布手段１１１は実施の形態１の電子財布手段１０１の持つ機能をすべて持つと同時に、暗号化手段１０５に対して電子価値情報を渡して登録電子価値情報を生成することと、登録電子価値情報を渡して電子価値情報を生成することを要求する機能を持つ。

【００８８】

電子金庫手段１１３は電子金庫手段１０３のソフトウェアを変更したものであり、電子金庫手段１１３は電子金庫記憶手段１１０の内容の参照と変更を行なうことができる。電子金庫１０３が登録電子価値情報２０３の登録要求を受けた場合、図５（ｂ）に示す登録証３０４を登録電子価値情報２０３を用いて生成する。登録証３０４を生成する処理の流れを以下に説明する。また、電子金庫手段１１３は、登録電子価値情報２０３からダイジェスト３０２を抽出する。また、暗号化電子価値情報２０２を一方向性のハッシュ関数に通してＸ２という数を生成

する。電子金庫手段１１３が持つカウンタを参照しＹ２という数を取得する。前記カウンタは参照の度に１ずつ昇順で増加し、上限に達すれば０に戻るものであるとする。これらダイジェスト３０２とハッシュ値Ｘ２とカウンタ値Ｙ２を組として登録証３０４とする。前記Ｘ２を生成するために用いたハッシュ関数として、ＭＤ５やＳＨＡ１などの分散性の高いものを用いることとする。登録証３０４はダイジェスト３０２の情報を含むため、それを参照することで登録された電子価値情報の概要を把握する事ができる。なお、ダイジェスト３０２は空情報の場合もあってもよいが、その場合は登録証からデンシカチジョウホウの概要を知る事はできない。

【００８９】

ユーザが端末１１２を操作して電子価値情報２０１をバックアップする手順を示す。以下の手順での選択動作はすべてユーザによって行なわれる。

(1-1) 端末１１２が、電子財布手段１１１に電子価値情報リストを要求する。電子財布手段１１１は電子価値情報のリストを生成し、端末１１２に送る。

(1-2) 端末１１２が、電子価値情報リストから選択した電子価値情報２０１を電子財布手段１１１に要求する。電子財布手段１１１は電子価値情報２０１を電子財布記憶手段１０２から取得する。暗号化手段１０５は電子価値情報２０１から登録電子価値情報２０３を生成し、電子財布手段１１１に送る。電子財布手段１１１は登録電子価値情報２０３を端末１１２に送る。

(1-3) 端末１１２が、登録電子価値情報２０３の登録を電子金庫手段１１３に要求する。電子金庫手段１１３は登録電子価値情報２０３を電子金庫記憶手段１１０に保管すると同時に、登録電子価値情報２０３から登録証３０４を生成し、登録証３０４を端末１１２に送る。

(1-4) 端末１１２が、登録証３０４の保管を電子財布手段１１１に要求する。電子財布手段１１１は登録証３０４を電子財布記憶手段１０２に保管し、完了通知を端末１１２に送る。

【００９０】

同様に、ユーザが端末１１２を操作して電子財布記憶手段１０２に保管された登録証３０４に対応する電子価値情報２０１を電子財布記憶手段１０２上に復元

する手順を次に示す。

(2-1) 端末１１２が、電子財布手段１１１に登録証リストを要求する。電子財布手段１１１は登録証リストを生成し、端末１１２に送る。

(2-2) 端末１１２が、登録証リストから選択した登録証３０４を電子財布手段１１１に要求する。電子財布手段１１１は登録証３０４を電子財布記憶手段１０２から取得し、端末１１２に送る。

(2-3) 端末１１２が、電子金庫手段１１３に登録証３０４を提示し、対応する登録電子価値情報を要求する。電子金庫手段１１３は登録証３０４を用いて登録電子価値情報２０３を検索して取得し、端末１１２に送る。

(2-4) 端末１１２が、登録電子価値情報２０３の登録を電子財布手段１１１に要求する。電子財布手段１１１は登録電子価値情報２０３を暗号化手段１０５に送り、電子価値情報２０１を取得し、電子財布記憶手段１０２に保管し、完了通知を取得する。

【００９１】

以上に説明したシステムを用いることで、ユーザが持つ電子価値情報を電子金庫手段には秘密の鍵を用いて暗号化してバックアップすることと、バックアップした電子価値情報の概要をローカルで把握することと、必要に応じて暗号化してバックアップした電子価値情報を電子金庫手段から復元することが可能となる。

【００９２】

【実施の形態３】

図８から９を用いて、請求項４と請求項６と請求項１２と請求項４３から請求項４４と請求項４８の実施の形態について述べる。図８は本実施の形態における電子価値情報バックアップシステムの一例を示した構成図であり、本システムは実施の形態２（図４）で示されたシステムの端末１１２を端末１１４に変更し、ＩＣカード１２２をＩＣカード１２３に変更して暗号化手段１０５を暗号化手段１１５に変更し、鍵管理手段１０６を追加したものである。

【００９３】

端末１１４と暗号化手段１１５はそれぞれ、端末１１２と暗号化手段１０５の間で通信を行なえるように変更したものであり、それを除いた機能は端末１１２

と暗号化手段１０５と同様である。鍵管理手段１０６はワークステーションまたはパーソナルコンピュータなどのコンピュータ装置と、前記コンピュータシステム上で動作するソフトウェアから構成される。鍵管理手段１０６は鍵管理記憶手段１１６の内容の参照と変更を行なうことができる。鍵管理記憶手段１１６は鍵管理手段１０６が内容の参照と変更を行なうことができる記憶装置であり、ハードディスクなどで実現される。鍵管理記憶手段１１６上には前記コンピュータシステムのＯＳが管理するファイルシステムが構築されている。

【００９４】

図９に鍵管理記憶手段１１６での情報の保管方法を示す。鍵管理記憶手段１１６は、鍵情報４９１をファイル８０３、認証情報８９１をファイル８０４として保管する。ファイル８０３へのパスとファイル８０４へのパスと前記認証情報のハッシュ値を組として、インデックスファイル８５３の１つのエントリとして登録する。インデックスファイル８５３は１エントリ１行のＣＳＶファイルであり、各行はハッシュ値によって昇順にソートされている。端末１１４から鍵管理手段１０６に認証情報８９１が提示された場合に、インデックスファイル８５３から認証情報８９１のハッシュ値に一致するエントリ群を検索し、その中から認証情報が完全に一致するエントリを抽出する。これにより、認証情報８９１に対応する鍵情報４９１を検索することが可能である。

【００９５】

本実施の形態では、前記の認証情報８９１として端末１１４から入力したパスワードを用いる。なお、認証情報８９１として、ＩＣカード１２３の固有ＩＤ、または鍵保管手段１０４が保持する暗号鍵４０１を用いて復号鍵４０２を暗号化したものを用いても良い。

【００９６】

電子価値情報のバックアップと復元の仕組みは実施の形態２と同様であるので説明を省略する。例えば、鍵保管手段１０４に保持されている復号鍵４０２をバックアップする鍵情報４９１とした場合の鍵情報４９１のバックアップと復元の手順について説明する。なお、鍵情報４９１として、暗号鍵４０１と復号鍵４０２の組を用いてもよい。

【００９７】

ユーザが端末１１４を操作して復号鍵４０２をバックアップする手順を示す。以下の手順での選択動作はすべてユーザによって行なわれる。

(1-1) 端末１１４が暗号化手段１１５に対して復号鍵の取得を要求する。

(1-2) 暗号化手段１１５が鍵保管手段１０４を参照し、復号鍵４０２を取得する。

(1-3) 暗号化手段１１５が端末１１４に復号鍵４０２を渡す。

(1-4) 端末１１４が認証情報８９１を取得する。本実施の形態ではパスワード入力をユーザに行なわせる。

(1-5) 端末１１４が復号鍵４０２を鍵管理手段１０６に認証情報８９１とともに登録することを要求する。

(1-6) 鍵管理手段１０６が復号鍵４０２と認証情報８９１を組として鍵管理記憶手段１１６に保管する。

(1-7) 鍵管理手段１０６が端末１１４に登録完了を通知する。

【００９８】

同様に、ユーザが端末１１４を操作して鍵管理記憶手段１１６に保管された復号鍵４４０２を鍵保管手段１０４に復元する手順を次に示す。

(2-1) 端末１１４が認証情報８９１を取得する。本実施の形態ではパスワード入力をユーザに行なわせる。

(2-2) 端末１１４が鍵管理手段１０６に認証情報８９１を提示して、復号鍵の取得を要求する。

(2-3) 鍵保管手段１０６は認証情報に対応する復号鍵４０２を鍵管理記憶手段１１６から抽出し、端末１１４に渡す。

(2-4) 端末１１４が復号鍵４０２を暗号化手段１０５に送る。

(2-5) 暗号化手段１１５が復号鍵４０２を鍵保管手段１０４に保管する。

(2-6) 暗号化手段１１５が復号鍵の復元が完了したことを端末１００に通知する。

【００９９】

なお、暗号鍵４０１と復号鍵４０２の鍵ペアを鍵管理手段１０６で生成し、鍵

保管手段１０４に配布してもよい。この場合、復号鍵の４０２のバックアップは鍵ペアの配布時に同時に行なわれる。この場合の鍵ペア配布の手順は次の通りである。

(3-1) 端末１１４が認証情報８９１を取得する。

(3-2) 端末１１４が認証情報８９１を鍵管理手段１０６に送るとともに、暗号鍵と復号鍵の新規生成を要求する。

(3-3) 鍵管理手段１０６が、暗号鍵４０１と復号鍵４０２を生成する。

(3-4) 鍵管理手段１０６が、復号鍵４０２と認証情報８９１を組として鍵管理記憶手段１１６に保管する。

(3-5) 鍵管理手段１０６が、暗号鍵４０１と復号鍵４０２の鍵ペアを端末１１４に送る。(3-6) 端末１１４が暗号化手段１１５に前記鍵ペアを鍵保管手段１０４に登録することを要求する。

(3-7) 暗号化手段１１５が鍵保管手段１０４に前記鍵ペアを保管する。

(3-8) 暗号化手段１１５が端末１１４に前記鍵ペアの保管完了を通知する。

【０１００】

以上に説明したシステムを用いることで、ユーザが持つ電子価値情報を電子金庫手段には秘密の鍵を用いて暗号化してバックアップすることと、バックアップした電子価値情報の概要をローカルで把握することと、必要に応じて暗号化してバックアップした電子価値情報を電子金庫手段から復元することと、前記の暗号化を解読する復号鍵を紛失した場合にも認証が成功すればその鍵を鍵保管手段上に復元することで暗号化された電子価値情報を復号することが可能となる。

【０１０１】

【実施の形態４】

図１７から１８を用いて、請求項７から８と請求項３１から請求項３２と請求項４１から請求項４２と請求項４９の実施の形態について述べる。図１７は本実施の形態に置ける電子価値情報バックアップシステムの一例を示した構成図であり、本システムは実施の形態３（図８）で示されたシステムの端末１１４を端末１４１に置き換え、電子金庫手段１１３を電子金庫手段１４２に置き換え、ＩＣカード１２３をＩＣカード１２５に置き換え、電子財布手段１１１を電子財布手

段１３９に変更し、暗号化手段１１５を暗号化手段１４０に変更したものである。

【０１０２】

暗号化手段１４０は、暗号化手段１１５の鍵情報バックアップと復元の仕組みを変更したものであり、鍵情報のバックアップと復元時に、電子財布手段１３９と連携するようにしたものである。

【０１０３】

電子金庫手段１４２は、電子金庫手段１１３が電子金庫記憶手段１１０に保管し管理するデータのデータ形式を変更したものである。そのデータ形式の例を図１８の登録電子価値情報２０４に示す。この登録電子価値情報２０４は、電子財布手段１３９から電子価値情報２０１を受けとった暗号化手段１４０が生成する。鍵情報が正常な場合の電子価値情報をバックアップから電子財布記憶手段に復元する手順は、実施の形態３と同様である。

【０１０４】

本実施の形態での鍵情報のバックアップの手順は、実施の形態３での鍵情報バックアップの手順を変更し、鍵管理手段１０６にバックアップする鍵情報４９１を分割復号鍵４０５としたものである。

(1-1) 端末１４１が暗号化手段１４０に対して復号鍵の取得を要求する。

(1-2) 暗号化手段１４０が鍵保管手段１０４を参照し、復号鍵４０２を取得する。

(1-3) 暗号化手段１４０が、復号鍵４０２を２つに分割して分割復号鍵４０５と分割復号鍵４０６を生成する。

(1-4) 暗号化手段１４０が端末１４１に分割復号鍵４０５を渡す。

(1-5) 端末１４１が認証情報８９１を取得する。本実施の形態ではパスワード入力をユーザに行なわせる。

(1-6) 端末１４１が分割復号鍵４０５を鍵管理手段１０６に認証情報８９１とともに登録することを要求する。

(1-7) 鍵管理手段１０６が分割復号鍵４０５と認証情報８９１を組として鍵管理記憶手段１１６に保管する。

(1-8) 鍵管理手段１０６が端末１４１に登録完了を通知する。

【０１０５】

本実施の形態での電子価値情報のバックアップの手順は、実施の形態２での電子価値情報のバックアップの手順を変更したものである。その手順を以下に示す。

(2-1) 端末１４１が、電子財布手段１３９に電子価値情報リストを要求する。電子財布手段１３９は電子価値情報のリストを生成し、端末１４１に送る。

(2-2) 端末１４１が、電子価値情報リストから選択した電子価値情報２０１を電子財布手段１３９に要求する。電子財布手段１３９は電子価値情報２０１を電子財布記憶手段１０２から取得する。暗号化手段１０５は電子価値情報２０１から登録電子価値情報２０４を生成し、電子財布手段１３９に送る。電子財布手段１３９は登録電子価値情報２０４を端末１４１に送る。

(2-3) 端末１４１が、登録電子価値情報２０４の登録を電子金庫手段１４２に要求する。電子金庫手段１４２は登録電子価値情報２０４を電子金庫記憶手段１１０に保管すると同時に、登録電子価値情報２０４から登録証３０４を生成し、登録証３０４を端末１４１に送る。

(2-4) 端末１４１が、登録証３０４の保管を電子財布手段１３９に要求する。電子財布手段１３９は登録証３０４を電子財布記憶手段１０２に保管し、完了通知を端末１４１に送る。

【０１０６】

本実施の形態での鍵情報の復元手順を以下に示す。

(3-1) 端末１４１が認証情報８９１を取得する。本実施の形態ではパスワード入力をユーザに行なわせる。

(3-2) 端末１４１が鍵管理手段１０６に認証情報８９１を提示して、分割復号鍵の取得を要求する。

(3-3) 鍵保管手段１０６は認証情報に対応する分割復号鍵４０５を鍵管理記憶手段１１６から抽出し、端末１４１に渡す。

(3-4) 端末１４１が分割復号鍵４０５を暗号化手段１４０に送る。

(3-5) 端末１４１が、電子財布手段１３９に登録証リストを要求する。電子財布

手段１３９は登録証リストを生成し、端末１４１に送る。

(3-6) 端末１４１が、登録証リストから選択した登録証３０４を電子財布手段１３９に要求する。電子財布手段１３９は登録証３０４を電子財布記憶手段１０２から取得し、端末１４１に送る。

(3-7) 端末１４１が、電子金庫手段１４２に登録証３０４を提示し、対応する登録電子価値情報を要求する。電子金庫手段１４２は登録証３０４を用いて登録電子価値情報２０４を検索して取得し、端末１４１に送る。

(3-8) 端末１４１が、登録電子価値情報２０４を電子財布手段１３９に送る。電子財布手段１３９は登録電子価値情報２０４から分割復号鍵４０６を取りだし、暗号化手段１０４に送る。

(3-9) 暗号化手段１４０が分割復号鍵４０５と分割復号鍵４０６を合成し、復号鍵４０２を取得する。

(3-10) 暗号化手段１４０が復号鍵４０２を鍵保管手段１０４に保管する。

(3-11) 暗号化手段１４０が復号鍵の復元が完了したことを端末１４１に通知する。

【０１０７】

なお、本実施の形態では、復号鍵を分割したものの一方をそれぞれを鍵管理記憶手段１１６に登録し、残りを電子金庫記憶手段１１０上の登録電子価値情報の中に埋め込むことによって鍵情報を分散してバックアップしている。復号鍵を分割したものをもちいるのではなく、復号鍵を数学的に生成するために用いる元の情報、例えば２つの素数をそれぞれ分割鍵として、一方を鍵管理記憶手段１１６に保管し、もう一方を電子金庫記憶手段１１０上の登録電子価値情報の中に埋め込むようにし、鍵の復元時に二つの情報をあわせて、暗号化手段１４０上で復号鍵を生成しなおすという方法を用いてもよい。この方法の場合、分割して保管した両方の元情報がわかっても、暗号化方式や鍵を生成するために用いるパラメータがわからない限り、鍵を生成することができない。

【０１０８】

以上に説明したシステムを用いることで、ユーザが持つ電子価値情報を電子金庫手段には秘密の鍵を用いて暗号化してバックアップすることと、バックアップ

した電子価値情報の概要をローカルで把握することと、必要に応じて暗号化してバックアップした電子価値情報を電子金庫手段から復元することと、前記の暗号化を解読する復号鍵を紛失した場合にもその鍵を復元することと、鍵管理手段および電子金庫手段の共謀がなければそのどちらに対しても完全な復号鍵を知られないことと、鍵管理手段と電子金庫手段の共謀があっても暗号化方式と鍵の生成方法を知られない限り復号鍵を知られないことと、暗号化した電子価値情報を電子財布手段上に復元することが可能となる。

【０１０９】

【実施の形態５】

図１０を用いて、請求項１３から１４の実施の形態について述べる。図１０は本実施の形態に置ける電子価値情報バックアップシステムの一例を示した構成図であり、本システムは実施の形態２（図４）で示されたシステムの端末１１２を端末１１７に置き換え、認証手段１１８を追加したものである。本実施の形態は、実施の形態２において認証情報８９１として端末か１１２から入力されたパスワードを用いているのを、認証手段１１８から入力された認証情報を用いるように変更したものである。

【０１１０】

認証手段１１８はＩＣカードリーダを持ち、前記ＩＣカードリーダを用いて、ＩＣカード１２２とは異なる個人認証用ＩＣカードからＩＣカード所有者情報を取得する。前記ＩＣカード所有者情報を認証情報８９１として用いる。前記の個人認証用ＩＣカードとしては、運転免許証やパスポートなどの行政などが発行する信頼できるカードを用いる。なお、認証手段１１８が指紋読みとり装置を持ち、前記指紋読みとり装置がユーザ指紋情報を取得し、前記ユーザ指紋情報を認証情報８９１として用いてもよい。また、認証手段１１８がＩＣカードリーダと指紋読みとり装置をともに持ち、ＩＣカード所有者情報とユーザ指紋情報の組を認証情報８９１として用いてもよい。なお、指紋読みとり装置は、掌紋読みとり装置や網膜読みとり装置などの生体情報読みとり装置と置き換えてもよい。

【０１１１】

以上に説明したシステムを用いることで、ユーザが持つ電子価値情報を電子金

庫手段には秘密の鍵を用いて暗号化してバックアップすることと、バックアップした電子価値情報の概要をローカルで把握することと、必要に応じて暗号化してバックアップした電子価値情報を電子金庫手段から復元することと、前記の暗号化を解読する復号鍵を紛失した場合にも認証が成功すればその鍵を鍵保管手段上に復元することで暗号化された電子価値情報を復号することと、安全な方法で認証を実現することが可能となる。

【０１１２】

【実施の形態６】

図１１を用いて、請求項１５と請求項４５の実施の形態について述べる。図１１は本実施の形態における電子価値情報バックアップシステムの一例を示した構成図であり、本システムは実施の形態５（図１０）で示されたシステムの鍵管理手段１０６を鍵管理手段１１９に置き換え、電子金庫手段１１３を電子金庫手段１３１に置き換え、端末１１７を端末１３２に置き換えたものである。

【０１１３】

本実施の形態では、鍵管理手段１１９と電子金庫手段１３１はお互いに通信する。これによって、実施の形態５に対して、鍵保管手段１０４から復号鍵を紛失したような緊急時に電子価値情報をバックアップから復元する新しい方法が追加される。

【０１１４】

同様に、ユーザが端末１３２を操作して電子財布記憶手段１０２に保管された登録証３０４に対応する電子価値情報２０１を電子財布記憶手段１０２上に復元する手順を次に示す。以下、復元したい電子価値情報を電子価値情報２０１、対応する登録証を登録証３０１、電子金庫上での電子価値情報２０１に対応する暗号化電子価値情報である暗号化電子価値情報２０２を含んだ登録電子価値情報を電子価値情報２０３、前記暗号化電子価値情報の復号に必要な復号鍵を復号鍵４０２として説明する。

(1-1) 端末１３２が、登録証３０１を電子財布手段１１１から取得する（詳細の手順は実施の形態２と同様である）。

(1-2) 端末１３２が、認証情報８９１とともに登録証３０１を鍵管理手段１１９

に送る。(1-3) 鍵管理手段１１９が、認証情報８９１に対応する復号鍵４０２を鍵管理記憶手段１１６から抽出する。対応する鍵が見つからない場合はエラー通知を端末１３２に送る。

(1-4) 鍵管理手段１１９が、電子金庫手段１３１に登録証３０１に対応する登録電子価値情報の取得を要求する。

(1-5) 電子金庫手段１３１が、電子金庫記憶手段１１０から登録証３０１に対応する登録電子価値情報２０３を抽出する。

(1-6) 電子金庫手段１３１が、登録電子価値情報２０３を鍵管理手段１１９に返す。

(1-7) 鍵管理手段１１９が、登録電子価値情報２０３内の署名３０３を復号鍵４０２を用いて検証し、暗号化電子価値情報２０２を復号鍵４０２を用いて復号し、電子価値情報２０１を取得する。

(1-8) 鍵管理手段１１９が、電子価値情報２０１を端末１３２に返す。

(1-9) 端末１３２が、電子財布手段１１１に電子価値情報２０１を電子財布記憶手段１０２に登録することを要求する。

(1-10) 電子財布手段１１１が電子価値情報２０１を電子財布記憶手段１０２に登録し、復元の完了を端末１３２に通知する。

【０１１５】

なお、電子価値情報２０１の復元が完了した時に、対応する登録証３０１を削除してもよい。

【０１１６】

以上に説明したシステムを用いることで、ユーザが持つ電子価値情報を電子金庫手段には秘密の鍵を用いて暗号化してバックアップすることと、バックアップした電子価値情報の概要をローカルで把握することと、必要に応じて暗号化してバックアップした電子価値情報を電子金庫手段から鍵管理手段を経由して鍵管理手段上で復号化してから復元することと、前記の暗号化を解読する復号鍵を紛失した場合にもその鍵を復元することで暗号化した電子価値情報を復元することと、鍵保管手段の正当性を所有者と強く結び付けることと、正当な所有者以外が不正に復号鍵を鍵保管手段に復元できないこと、正当な所有者以外が不正に電子価

値情報を復元できないことと、暗号化してバックアップした電子価値情報を維持しつつ暗号鍵と復号鍵の鍵ペアを変更することと、鍵保管手段の破損による場合の復号鍵の復元が可能となる。

【０１１７】

【実施の形態７】

図１２を用いて、請求項１６と請求項４６の実施の形態について述べる。図１２は本実施の形態における電子価値情報バックアップシステムの一例を示した構成図であり、本システムは実施の形態６（図１１）で示されたシステムの鍵管理手段１１３を鍵管理手段１３４に置き換え、端末１３２を端末１３３に置き換えたものである。

【０１１８】

本実施の形態における電子価値情報のバックアップと復元、復号鍵のバックアップと復元は、実施の形態３と同様である。本実施の形態は、鍵保管手段１０４上の暗号鍵と復号鍵がともに破損・消失した場合に、電子金庫手段１３１にバックアップされている電子価値情報を鍵管理手段１３４が取得し、鍵管理記憶手段１３４に登録されている復号鍵を用いて復号化する。鍵管理手段１３４は新しく暗号鍵と復号鍵の鍵ペアを生成し、前記暗号鍵を用いて電子価値情報を暗号化しなおし、新しい鍵ペアを端末１３３を経由して鍵保管手段１０４上に配布する。以下にその詳細の手順を示す。

(1-1) 端末１３３が、全登録証群を電子財布手段１１１から取得する。

(1-2) 端末１３３が、認証情報８９１とともに前記全登録証群を鍵管理手段１３４に送る。

(1-3) 鍵管理手段１１９が、認証情報８９１に対応する復号鍵４０２を鍵管理記憶手段１１６から抽出する。対応する鍵が見つからない場合はエラー通知を端末１３４に送る。

(1-4) 鍵管理手段１３４が、電子金庫手段１３１に前記全登録証群に対応する暗号化電子価値情報すべての取得を要求する。

(1-5) 電子金庫手段１３１が、電子金庫記憶手段１１０から前記全登録証群に対応する暗号化電子価値情報群を抽出する。

(1-6) 電子金庫手段１３１が、登録電子価値情報群を鍵管理手段１３４に返す。

(1-7) 鍵管理手段１３４が、登録電子価値情報群に含まれるすべての暗号化電子価値情報を復号鍵４０２を用いて復号し、電子価値情報群を取得する。

(1-8) 鍵管理手段１３４が、暗号鍵４０３と復号鍵４０４の鍵ペアを生成する。

(1-9) 鍵管理手段１３４が、暗号鍵４０３で全電子価値情報群を暗号化し、新しい暗号化電子価値情報群を生成し、登録電子価値情報群に含まれる署名も新しい暗号鍵で生成し直し置き換える。

(1-10) 鍵管理手段１３４が、新しい登録電子価値情報群を(1-5)で取得した登録電子価値情報群との置き換えることを電子金庫手段１３１に要求する。

(1-11) 電子金庫手段１３１が、古い登録電子価値情報群を新しい登録電子価値情報群で置き換え、その置換えの完了を鍵管理手段１３４に通知する。

(1-12) 鍵管理手段１３４が、鍵管理記憶手段１１６上に保管された復号鍵４０２を復号鍵４０４に置き換える。

(1-13) 鍵管理手段１３４が、暗号鍵４０３と復号鍵４０４の鍵ペアを端末１３３に送る。

(1-14) 端末１３３が、暗号化手段１１５に前記鍵ペアを鍵保管手段１０４に保管するよう要求する。

(1-15) 暗号化手段１１５が、鍵保管手段１０４に前記鍵ペアを保管し、その完了を通知する。

【０１１９】

以上に説明したシステムを用いることで、ユーザが持つ電子価値情報を電子金庫手段には秘密の鍵を用いて暗号化してバックアップすることと、バックアップした電子価値情報の概要をローカルで把握することと、必要に応じて暗号化してバックアップした電子価値情報を電子金庫手段から鍵管理手段を経由して鍵管理手段上で復号化してから復元することと、前記の暗号化を解読する復号鍵を紛失した場合にもその鍵を復元することで暗号化した電子価値情報を復元することと、鍵保管手段の正当性を所有者と強く結び付けることと、正当な所有者以外が不正に復号鍵を鍵保管手段に復元できないこと、正当な所有者以外が不正に電子価値情報を復元できないことと、暗号化してバックアップした電子価値情報を維持

しつつ暗号鍵と復号鍵の鍵ペアを変更することと、鍵保管手段の破損による場合の復号鍵の復元が可能となる。

【０１２０】

【実施の形態８】

図１３を用いて、請求項１７と請求項４７の実施の形態について述べる。図１３は本実施の形態における電子価値情報バックアップシステムの一例を示した構成図であり、本システムは実施の形態６（図１１）で示されたシステムの鍵管理手段１３４を鍵管理手段１３６に置き換え、端末１３３を端末１３５に置き換えたものである。

【０１２１】

本実施の形態の鍵管理手段１３６は、実施の形態６の鍵管理手段１３４が復号化した電子価値情報を端末１３３経由で送っていたのとは違い、新しく生成した暗号鍵で暗号化した状態で電子価値情報を端末１３５経由で送り、新しい暗号鍵と復号鍵を配布することを特徴としている。

(1-1) 端末１３５が、全登録証群を電子財布手段１１１から取得する。

(1-2) 端末１３５が、認証情報８９１とともに前記全登録証群を鍵管理手段１３６に送る。

(1-3) 鍵管理手段１１９が、認証情報８９１に対応する復号鍵４０２を鍵管理記憶手段１１６から抽出する。対応する鍵が見つからない場合はエラー通知を端末１３５に送る。

(1-4) 鍵管理手段１３６が、電子金庫手段１３１に前記全登録証群に対応する暗号化電子価値情報すべての取得を要求する。

(1-5) 電子金庫手段１３１が、電子金庫記憶手段１１０から前記全登録証群に対応する暗号化電子価値情報群を抽出する。

(1-6) 電子金庫手段１３１が、登録電子価値情報群を鍵管理手段１３６に返す。

(1-7) 鍵管理手段１３６が、登録電子価値情報群中の署名を検証した後、すべての暗号化電子価値情報を復号鍵４０２を用いて復号し、電子価値情報群を取得する。

(1-8) 鍵管理手段１３６が、暗号鍵４０３と復号鍵４０４の鍵ペアを生成する。

(1-9) 鍵管理手段１３６が、暗号鍵４０３で全電子価値情報群を暗号化し、新しく暗号化電子価値情報群を生成する。

(1-10) 鍵管理手段１３６が、鍵管理記憶手段１１６上に保管された復号鍵４０２を復号鍵４０４に置き換える。

(1-11) 鍵管理手段１３６が、暗号鍵４０３と復号鍵４０４の鍵ペアを端末１３５に送る。

(1-12) 鍵管理手段１３６が、電子金庫手段１３１上の(1-5)で取得した暗号化電子価値情報群を含む登録電子価値情報群の削除を要求する。

(1-13) 電子金庫手段１３１が、要求された登録電子価値情報群を削除し、その完了を鍵管理手段１３６に通知する。

(1-14) 鍵管理手段１３６が、新しい暗号化電子価値情報群を端末１３５に送る。

(1-15) 端末１３５が、新しい暗号化電子価値情報群と前記鍵ペアを暗号化手段１１５に送る。

(1-16) 暗号化手段１１５が前記鍵ペアを鍵保管手段１０４に保管する。

(1-17) 暗号化手段１１５が新しい暗号化電子価値情報群を復号鍵４０４で復号化し、電子財布手段１１１に電子価値情報群を送る。

(1-18) 電子財布手段１１１が電子価値情報群を電子財布記憶手段１０２上に復元する。(1-19) 電子財布手段１１１が端末１３５に完了を通知する。

【０１２２】

以上に説明したシステムを用いることで、ユーザが持つ電子価値情報を電子金庫手段には秘密の鍵を用いて暗号化してバックアップすることと、バックアップした電子価値情報の概要をローカルで把握することと、必要に応じて暗号化してバックアップした電子価値情報を電子金庫手段から鍵管理手段を経由して鍵管理手段上で復号化してから復元することと、前記の暗号化を解読する復号鍵を紛失した場合にもその鍵を復元することで暗号化した電子価値情報を復元することと、鍵保管手段の正当性を所有者と強く結び付けることと、正当な所有者以外が不正に復号鍵を鍵保管手段に復元できないこと、正当な所有者以外が不正に電子価値情報を復元できないことと、暗号化してバックアップした電子価値情報を維持

しつつ暗号鍵と復号鍵の鍵ペアを変更することと、鍵保管手段の破損による場合の復号鍵の復元が可能となる。

【０１２３】

【実施の形態９】

図１４から１６を用いて、請求項１８から２７と請求項３４から請求項３７の実施の形態について述べる。

【０１２４】

図１４は本実施の形態が示す電子価値情報バックアップシステムの一例を示した構成図である。これは実施の形態３のＩＣカード１２３をＩＣカード１２４に変更したものであり、ＩＣカード１２４はＩＣカード１２３の電子財布手段１１１を電子財布手段１３８に変更し、電子財布手段１３８と通信するバックアップ起動管理手段１０９を追加したものである。これによってバックアップする電子価値情報の選択を、ユーザによる手動選択ではなく事前に設定した条件に基づいて自動的に行なうようにしたものである。

【０１２５】

バックアップ起動管理手段１０９は、バックアップ条件情報を保持し、その条件情報に基づいて、バックアップする電子価値情報を決定する。本実施の形態では、バックアップ条件情報には初期設定が存在し、また条件情報をユーザが変更できるものとし、電子財布記憶手段１０２の空きメモリ容量、電子価値情報の有効期限、電子価値情報の種類、電子価値情報のサイズのそれぞれを組み合わせてバックアップ条件を設定することができるものとする。なお、電子価値情報が持つ情報の項目にあわせて、前記した以外の情報をバックアップ条件に用いても良い。

【０１２６】

バックアップ条件情報の例を図１５と図１６で示す。図１５は電子記憶手段上の電子価値情報群の例である。ここでバックアップ条件を映画のチケットとした場合、図１６（ａ）は前記バックアップ条件に対応する電子価値情報群を示す。本日の日付を2000年3月15日として、一ヶ月以内に使用可能な日がないことをバックアップ条件とした場合の対応する電子価値情報群は図１６（ｂ）がで示され

る。

【０１２７】

図３９はバックアップ起動管理手段１０９が管理するバックアップ条件をユーザが設定する手順を示した図であり、以下に示す番号順に実行される。以下の番号は、図３９における番号と対応している。

(1-1) 端末１３７がバックアップ起動手段１０９の現在のバックアップ条件を取得し、ユーザに提示する。

(1-2) ユーザはバックアップ条件を修正し、新しいバックアップ条件を生成する。

(1-3) 端末１３７がバックアップ起動手段１０９に新しいバックアップ条件を登録する。

【０１２８】

図４０はバックアップ手順を示した図であり、以下に示す番号順に実行される。以下の番号は、図４０における番号と対応する。

(2-1) (2-1)バックアップ起動管理手段１０９が電子財布手段１１に電子価値情報のリストを要求する。

(2-2) (2-2)電子財布手段１３８が電子財布記憶手段１０２を参照し、電子価値情報のリストを構成する。

(2-3) (2-3)電子財布手段１３８が電子価値情報のリストをバックアップ起動管理手段１０９に返す。

(2-4) (2-4)バックアップ起動管理手段１０９は登録されたバックアップ条件とリストを照合し、バックアップ対象電子価値情報リストを生成する。

(2-5) (2-5)バックアップ起動管理手段１０９は電子財布手段１３８にバックアップ対象電子価値情報リストを渡す。

(2-6) (2-6)電子財布手段１３８は電子財布記憶手段１０２からバックアップ対象電子価値情報リストで指定された電子価値情報群を取得する。

(2-7) (2-7)前記電子価値情報群に含まれるすべての電子価値情報をそれぞれ暗号化手段１１５を用いて暗号化し、暗号化電子価値情報群を生成する。

(2-8) (2-8)前記暗号化電子価値情報群に含まれるすべての暗号化電子価値情報

を端末１３７を経由して、電子金庫手段１１３にバックアップする。

(2-9) (2-9)電子金庫手段１１３から前記暗号化電子価値情報群に対応する登録証群を端末１３７を経由して電子財布手段１３８に渡す

(2-10) (2-10)電子財布手段１３８は前記登録証群を電子財布記憶手段１０２に保管し、電子財布記憶手段１０２上から前記電子価値情報群に含まれる電子価値情報をすべて削除する。

(2-11) (2-11)電子財布記憶手段１３８は端末１３７に完了を通知する。

【０１２９】

(2-8)、(2-9)、(2-10)での１つの暗号化電子価値情報に対しての手順の細部は、前述した実施の形態３と同様であるので、本実施の形態では詳細の説明を省略する。

【０１３０】

なお、一定時間ごとにバックアップ起動管理手段１０９が自動的に前記(2-1)から(2-11)で示した手順に従ってバックアップを開始してもよい。

【０１３１】

または新規の電子価値情報が電子財布記憶手段に登録される時やバックアップされていた電子価値情報を復元する時に、電子財布記憶手段１０２の記憶容量が不足する場合にバックアップ起動管理手段１０９が自動的に前記手順にしたがってバックアップを開始してもよい。

【０１３２】

またはユーザによる起動要求があった場合に、バックアップ起動管理手段１０９が自動的に前記手順にしたがってバックアップを開始してもよい。

【０１３３】

または、前記の条件の組み合わせによって、バックアップ起動管理手段１０９が自動的に前記手順にしたがってバックアップを開始してもよい。

【０１３４】

また、電子財布記憶手段の記憶容量不足の場合、現在の電子財布記憶手段に保持された電子価値情報をバックアップ条件情報に基づいてバックアップする処理を行なった上で新規の電子価値情報の登録やバックアップ済みの電子価値情報の

復元を継続することと、新規の電子価値情報の登録やバックアップ済み電子価値情報の復元を中断することと、手動で現在の電子財布記憶手段に保持された電子価値情報を選択しバックアップする処理を行なった上で新規の電子価値情報の登録やバックアップ済みの電子価値情報の復元を継続することを端末１３７を操作するユーザに選択させても良い。

【０１３５】

以上に説明したシステムを用いることで、ユーザが持つ電子価値情報を電子金庫手段には秘密の鍵を用いて暗号化してバックアップすることと、バックアップした電子価値情報の概要をローカルで把握することと、必要に応じて暗号化してバックアップした電子価値情報を電子金庫手段から復元することと、前記の暗号化を解読する復号鍵を紛失した場合にもその鍵を復元することで暗号化した電子価値情報を復元することと、鍵保管手段の正当性を所有者と強く結び付けることと、正当な所有者以外が不正に復号鍵を鍵保管手段に復元できないことと、鍵保管手段の破損による場合の復号鍵の復元することと、工場設定やユーザ設定に基づいて電子価値情報のバックアップが自動的に起動させることが可能となる。

【０１３６】

【発明の効果】

以上のように本発明によれば、第１にローカルの電子価値情報を暗号化してサーバ上にバックアップする手段を備えたことにより、電子価値情報をサーバに隠蔽した状態でバックアップすることと、ローカルの電子価値情報が破損した場合にも電子価値情報を復元する効果が得られる。

【０１３７】

第２に暗号化した電子価値情報の復号鍵を電子価値情報のバックアップ先のサーバとは別のサーバにバックアップする手段を備えたことにより、ローカルの復号鍵が破損した場合にも復号鍵を復元する事によって暗号化した電子価値情報を復元する効果が得られる。

【０１３８】

第３に復号鍵を分割してそれぞれを別々にバックアップする手段を備えた事により、復号鍵の全体を知られる事なく、ローカルに復号鍵を復元する効果が得ら

れる。

【０１３９】

第４に復号鍵をバックアップしたサーバに、暗号化した電子価値情報を復号させて電子価値情報をローカルに復元する手段を備えた事により、ローカルデバイスが壊滅的に破損または紛失した場合にも、電子価値情報を復元する効果が得られる。

【０１４０】

第５に復号鍵をバックアップしたサーバに、暗号化した電子価値情報を復号させ、新しい暗号化を行なわせて登録しなおし、新しい鍵情報をローカル環境に再配布させる手段を備えたことにより、ローカル環境の鍵情報のみが破損または紛失した場合にも、ローカル環境に与える影響を小さく抑えた上でバックアップした電子価値情報を復元できる環境を再構築する効果が得られる。

【図面の簡単な説明】

【図１】

本発明の実施の形態１の電子価値情報バックアップシステムの構成を示すブロック図

【図２】

実施の形態１の電子価値情報とダイジェスト情報と登録証の例図

【図３】

実施の形態１の電子財布手段上での電子価値情報と登録証の管理方法の例図

【図４】

本発明の実施の形態２の電子価値情報バックアップシステムの構成を示すブロック図

【図５】

実施の形態２の登録電子価値情報と登録証の例図

【図６】

実施の形態２の鍵保管手段上での暗号鍵と復号鍵の保管方法の例図

【図７】

実施の形態１の電子金庫記憶手段での情報の保管方法の例図

【図８】

本発明の実施の形態３の電子価値情報バックアップシステムの構成を示すブロック図

【図９】

実施の形態３の鍵管理記憶手段上の鍵情報の管理方法の例図

【図１０】

本発明の実施の形態５の電子価値情報バックアップシステムの構成を示すブロック図

【図１１】

本発明の実施の形態６の電子価値情報バックアップシステムの構成を示すブロック図

【図１２】

本発明の実施の形態７の電子価値情報バックアップシステムの構成を示すブロック図

【図１３】

本発明の実施の形態８の電子価値情報バックアップシステムの構成を示すブロック図

【図１４】

本発明の実施の形態９の電子価値情報バックアップシステムの構成を示すブロック図

【図１５】

実施の形態９の電子価値情報群の例図

【図１６】

実施の形態９のバックアップ対象の電子価値情報群の例図

【図１７】

実施の形態４の鍵管理記憶手段上の鍵情報の管理方法の例図

【図１８】

実施の形態４の登録電子価値情報と登録証の例図

【符号の説明】

１００　端末

１０１　電子財布手段

１０２　電子財布記憶手段

１０３　電子金庫手段

１０４　鍵保管手段

１０５　暗号化手段

１０６　鍵管理手段

１０９　バックアップ起動管理手段

１１０　電子金庫記憶手段

１１１　電子財布手段

１１２　端末

１１３　電子金庫手段

１１４　端末

１１５　暗号化手段

１１６　鍵管理記憶手段

１１７　端末

１１８　認証手段

１１９　鍵管理手段

１２１　１０１と１０２を含むＩＣカード

１２２　１０２と１０４と１０５と１１１を含むＩＣカード

１２３　１０２と１０４と１１５と１１１を含むＩＣカード

１２４　１０２と１０４と１０９と１１５と１３８を含むＩＣカード

１２５　１０２と１０４と１３９と１４０を含むＩＣカード

１３１　電子金庫手段

１３２　端末

１３３　端末

１３４　鍵管理手段

１３５　端末

１３６　鍵管理手段

１３７　端末

１３８　電子財布手段

１３９　電子財布手段

１４０　暗号化手段

１４１　端末

１４２　電子金庫手段

２０１　電子価値情報例

２０２　２０１に対応した暗号化電子価値情報例

２０３　２０２に対応した登録電子価値情報例

２０４　２０４と４０６に対応した登録電子価値情報例

３０１　２０１に対応した登録証

３０２　２０１に対応したダイジェスト例

３０３　２０３に含まれる署名

３０４　２０３に対応した登録証

４０１　暗号鍵例

４０２　復号鍵例

４０３　暗号鍵例

４０４　復号鍵例

４０５　４０２の分割復号鍵

４０６　４０２の分割復号鍵

４９１　鍵情報

８０１　電子金庫記憶手段上のファイル例

８０２　電子金庫記憶手段上のファイル例

８０３　鍵管理記憶手段上のファイル例

８０４　鍵管理記憶手段上のファイル例

８５１　電子財布記憶手段上のインデックス例

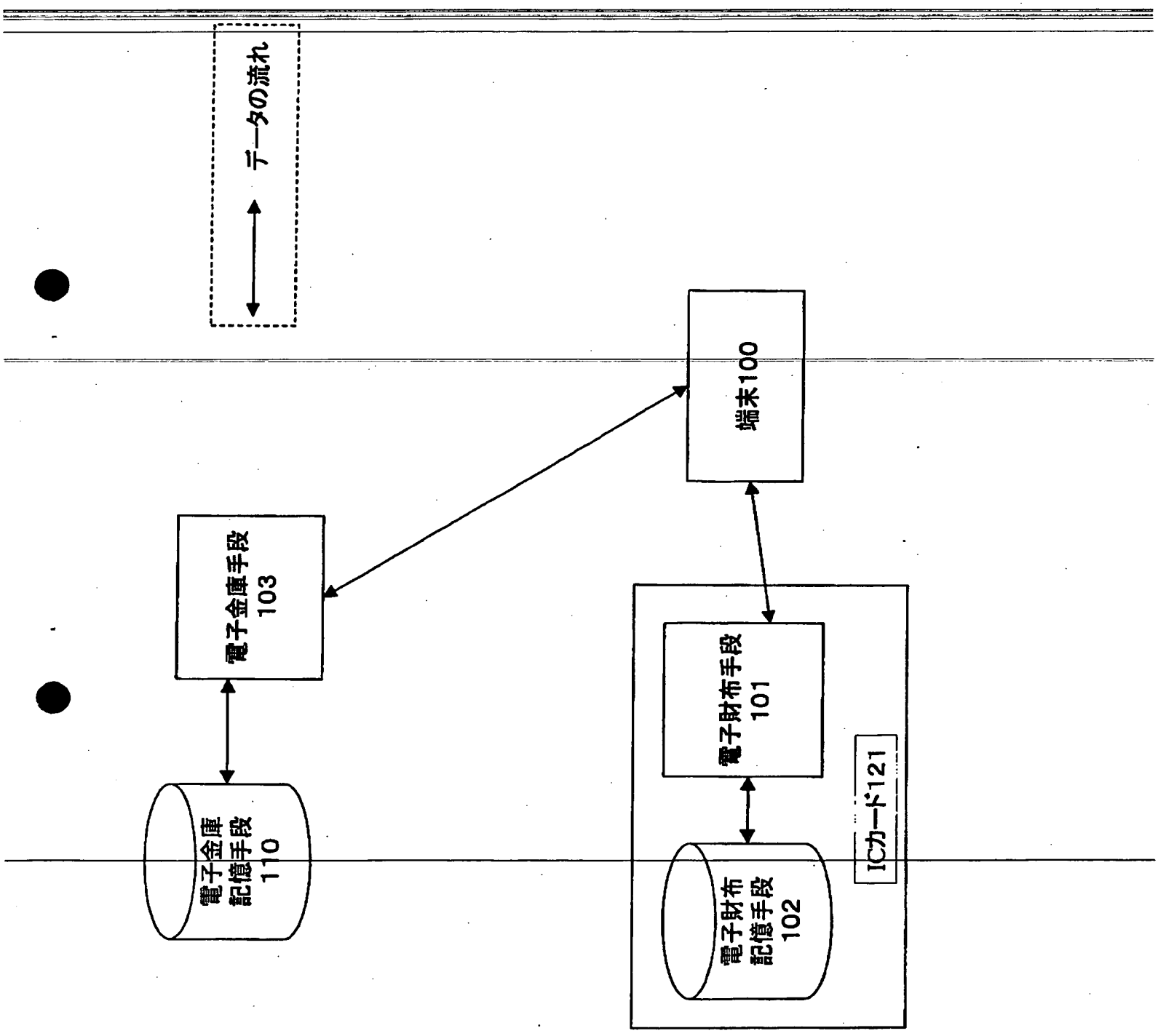
８５２　電子金庫記憶手段上のインデックスファイル例

８５３　電子金庫記憶手段上のインデックスファイル例

９１　認証情報例

【書類名】　　図面

【図１】



出証特２０００－３０６８１６２

【図２】

電子価値情報201

情報種別	映画チケット
名前	映画タイトル
単価	A円
数	B
合計金額	A×B円
場所	劇場名
有効期限	C～D
備考	……

(a)

ダイジェスト302

情報種別	映画チケット
名前	映画タイトル
数	B
有効期限	C～D
場所	劇場名

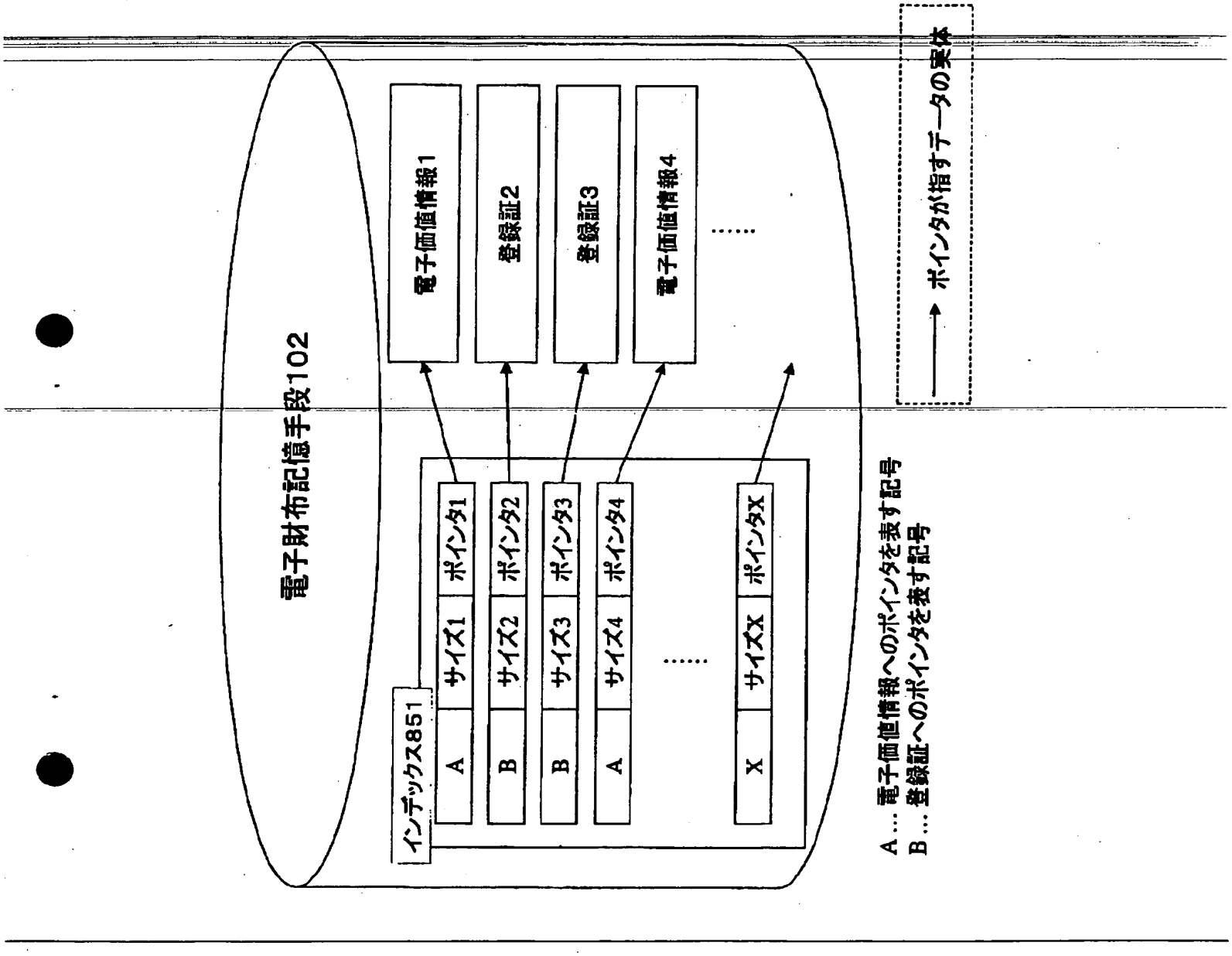
(b)

登録証301

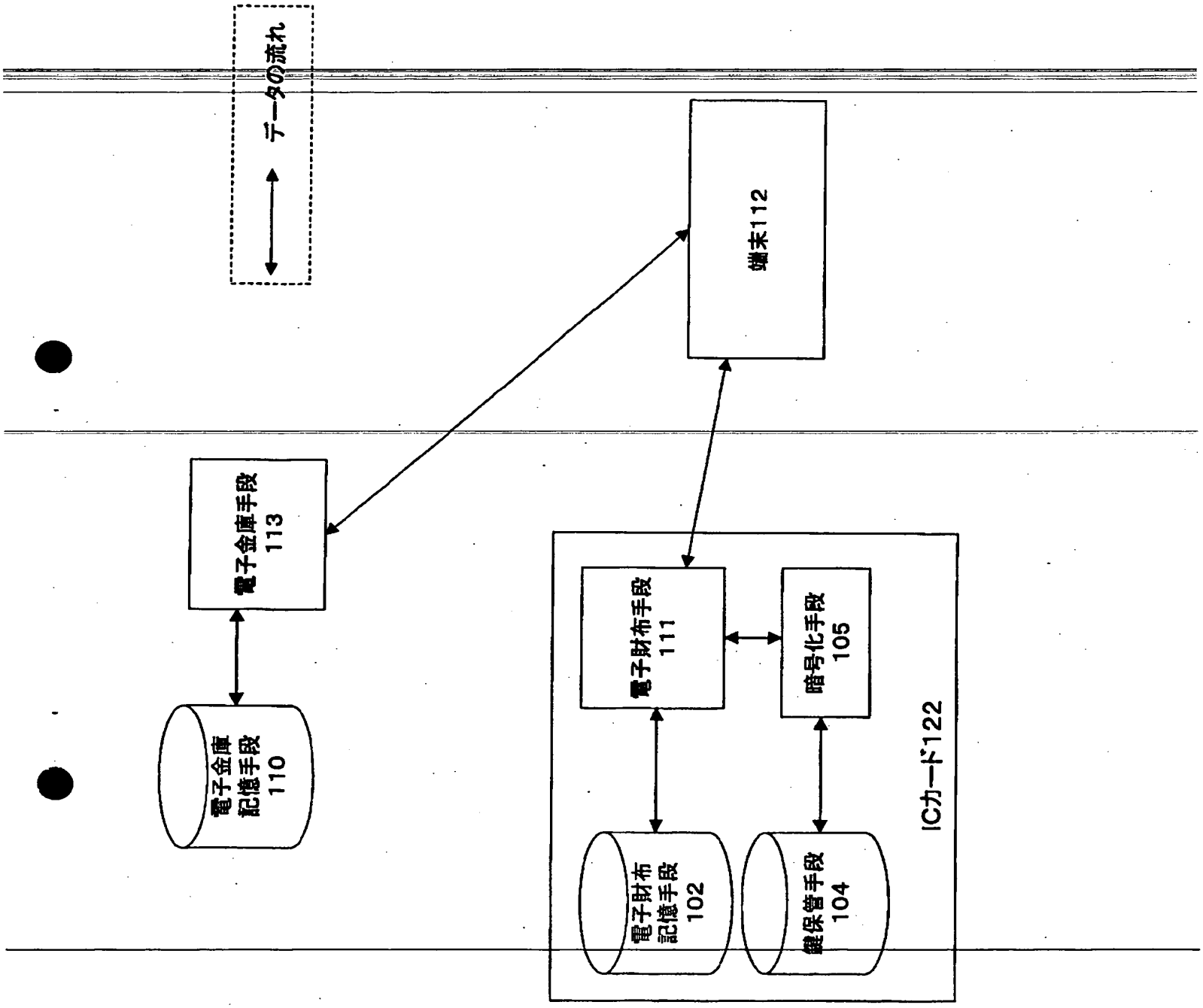
ダイジェスト302	ハッシュ値X1	カウンタ値Y1

(c)

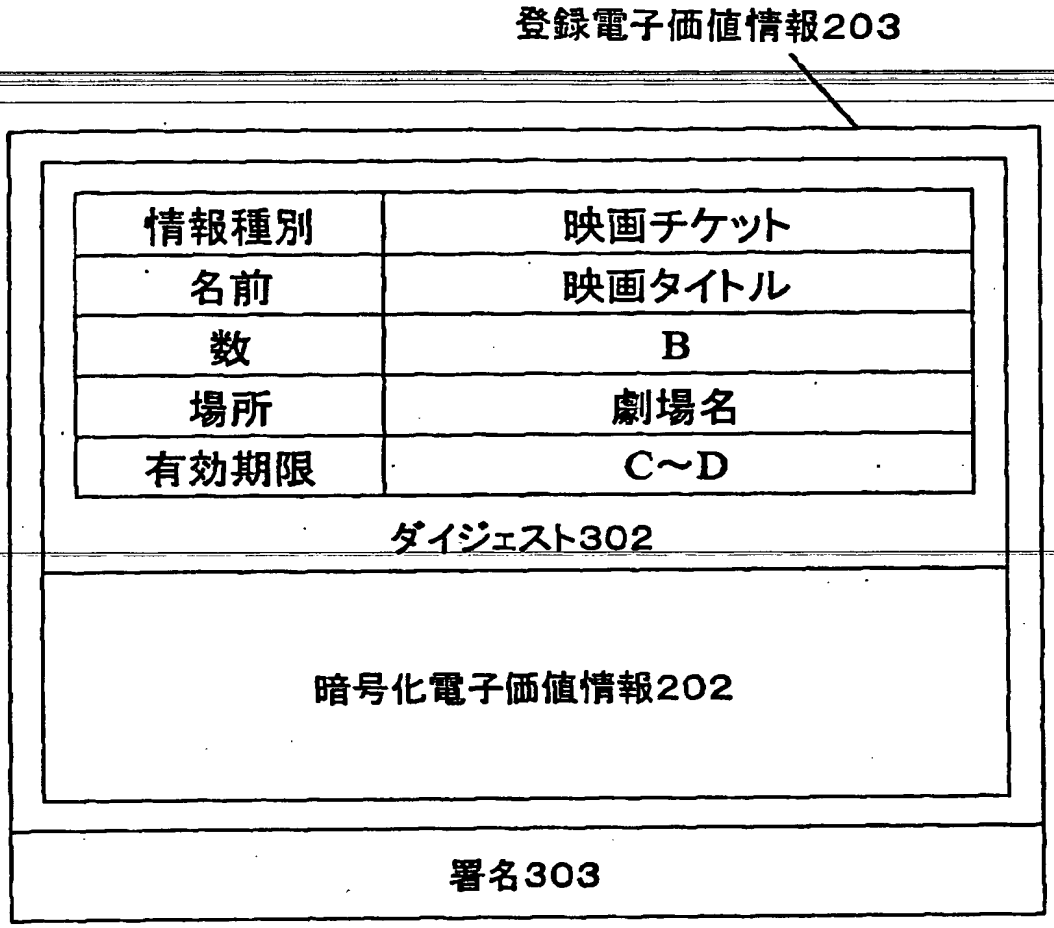
【図３】


電子財布記憶手段102
電子価値情報1
登録証2
登録証3
電子価値情報4
……
インデックス851
A
サイズ1
ポインタ1
B
サイズ2
ポインタ2
B
サイズ3
ポインタ3
A
サイズ4
ポインタ4
……
X
サイズX
ポインタX
ポインタが指すデータの実体
A…電子価値情報へのポインタを表す記号
B…登録証へのポインタを表す記号

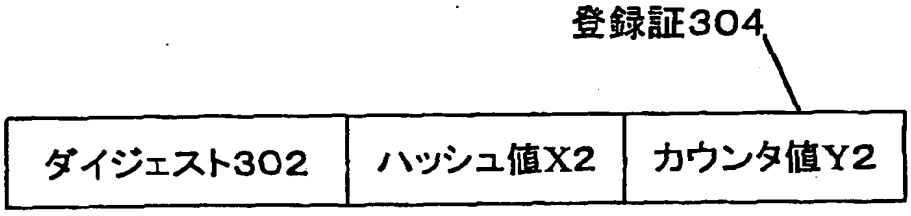
【図４】


データの流れ
端末112
電子金庫手段
113
電子金庫
記憶手段
110
電子財布手段
111
暗号化手段
105
ICカード122
電子財布
記憶手段
102
鍵保管手段
104

【図５】

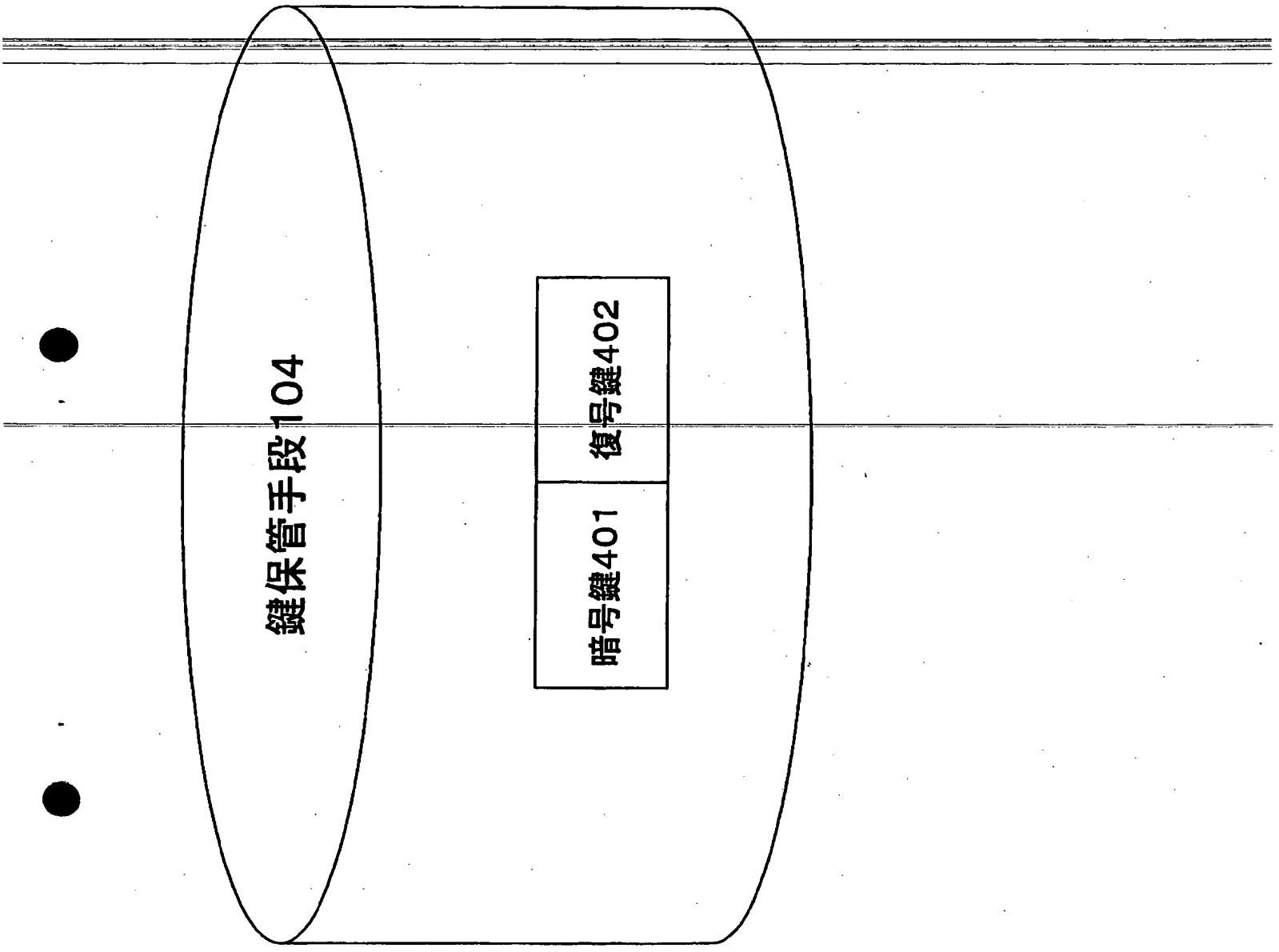

登録電子価値情報203
情報種別
映画チケット
名前
映画タイトル
数
B
場所
劇場名
有効期限
C～D
ダイジェスト302
暗号化電子価値情報202
署名303

(a)

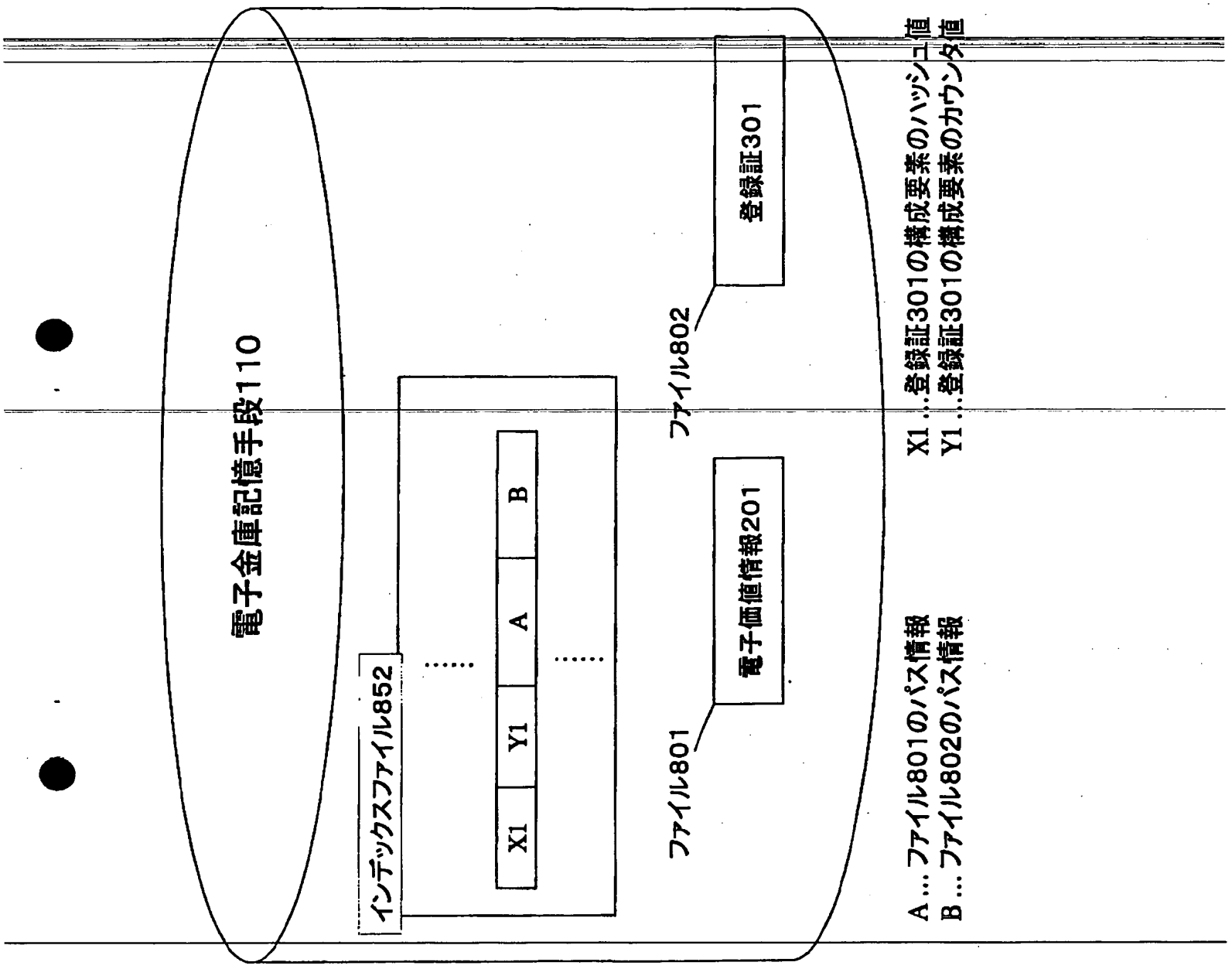

登録証304
ダイジェスト302
ハッシュ値X2
カウンタ値Y2

(b)

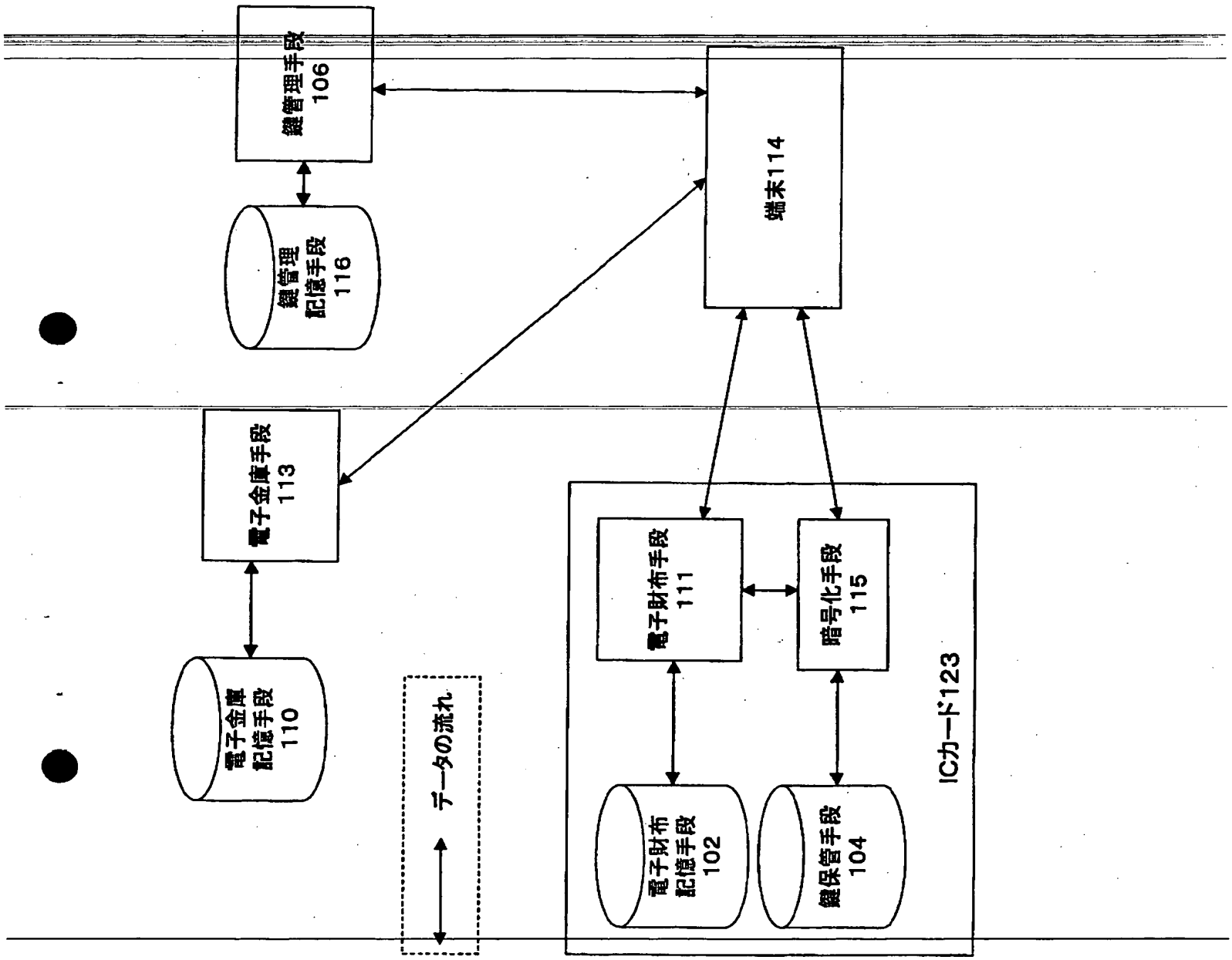
【図６】



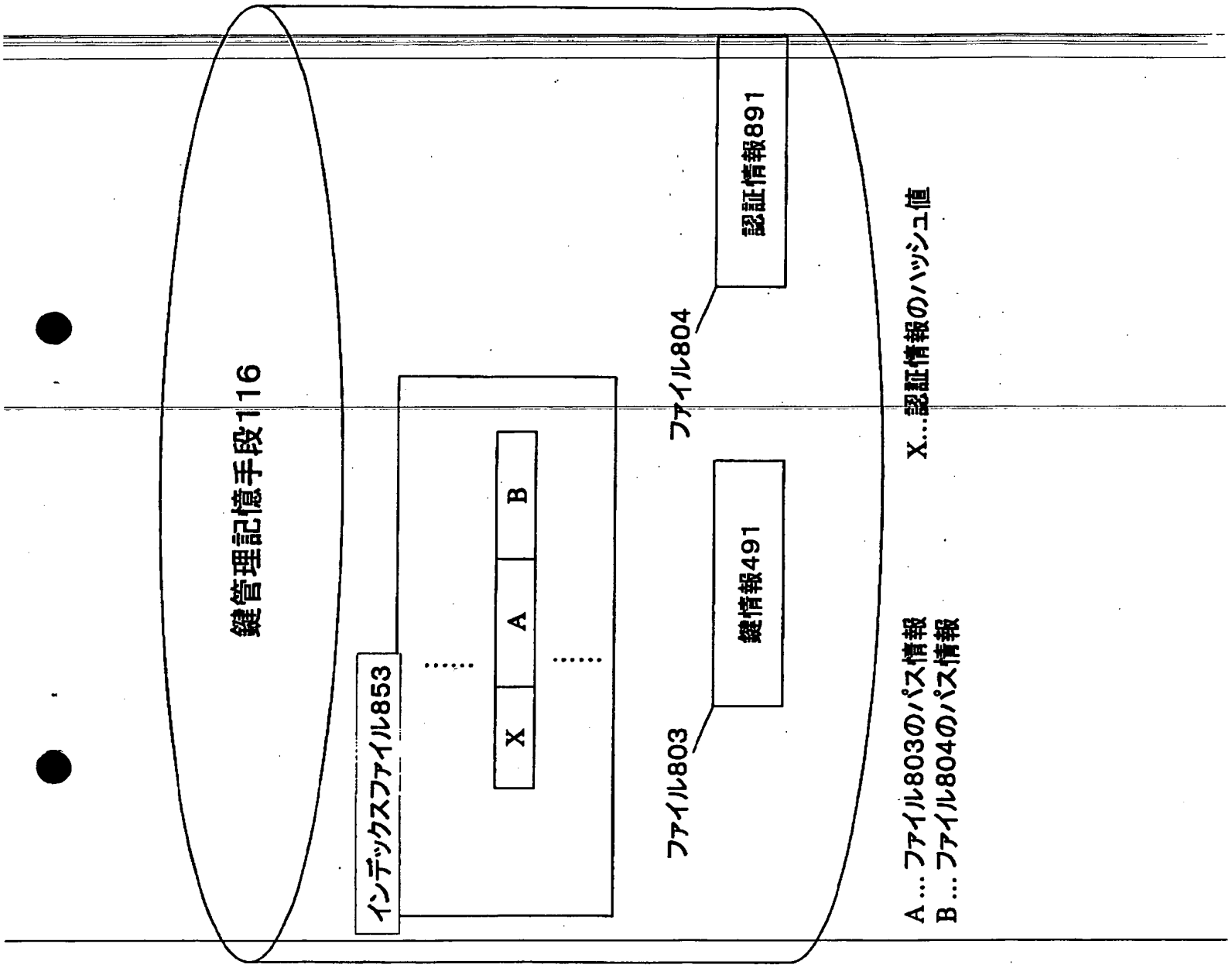
【図７】


電子金庫記憶手段110
インデックスファイル852
X1
Y1
A
B
ファイル801
電子価値情報201
ファイル802
登録証301
A…ファイル801のパス情報
B…ファイル802のパス情報
X1…登録証301の構成要素のハッシュ値
Y1…登録証301の構成要素のカウンタ値

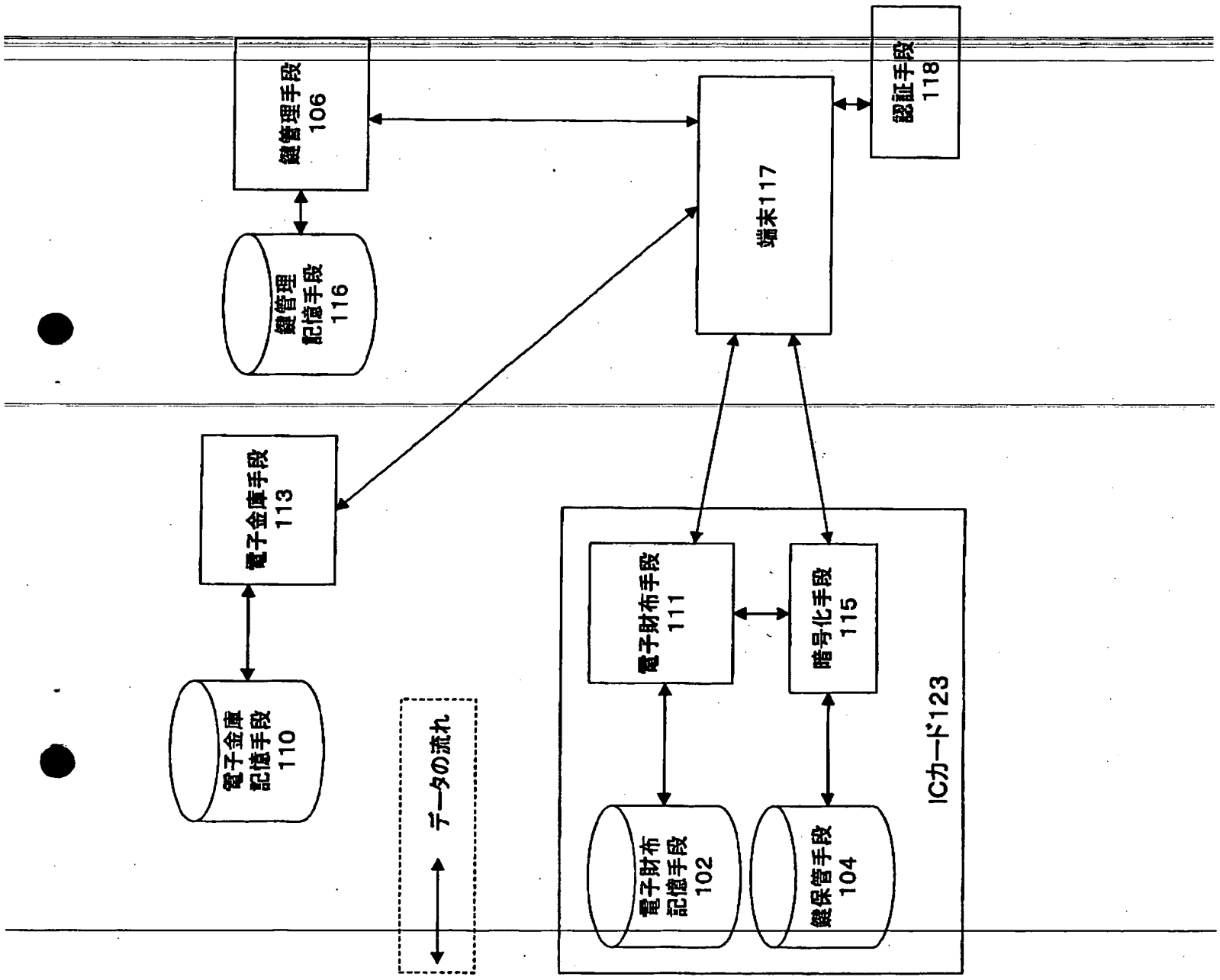
【図８】


鍵管理手段
106
端末114
鍵管理
記憶手段
116
電子金庫手段
113
電子金庫
記憶手段
110
データの流れ
電子財布手段
111
暗号化手段
115
ICカード123
電子財布
記憶手段
102
鍵保管手段
104

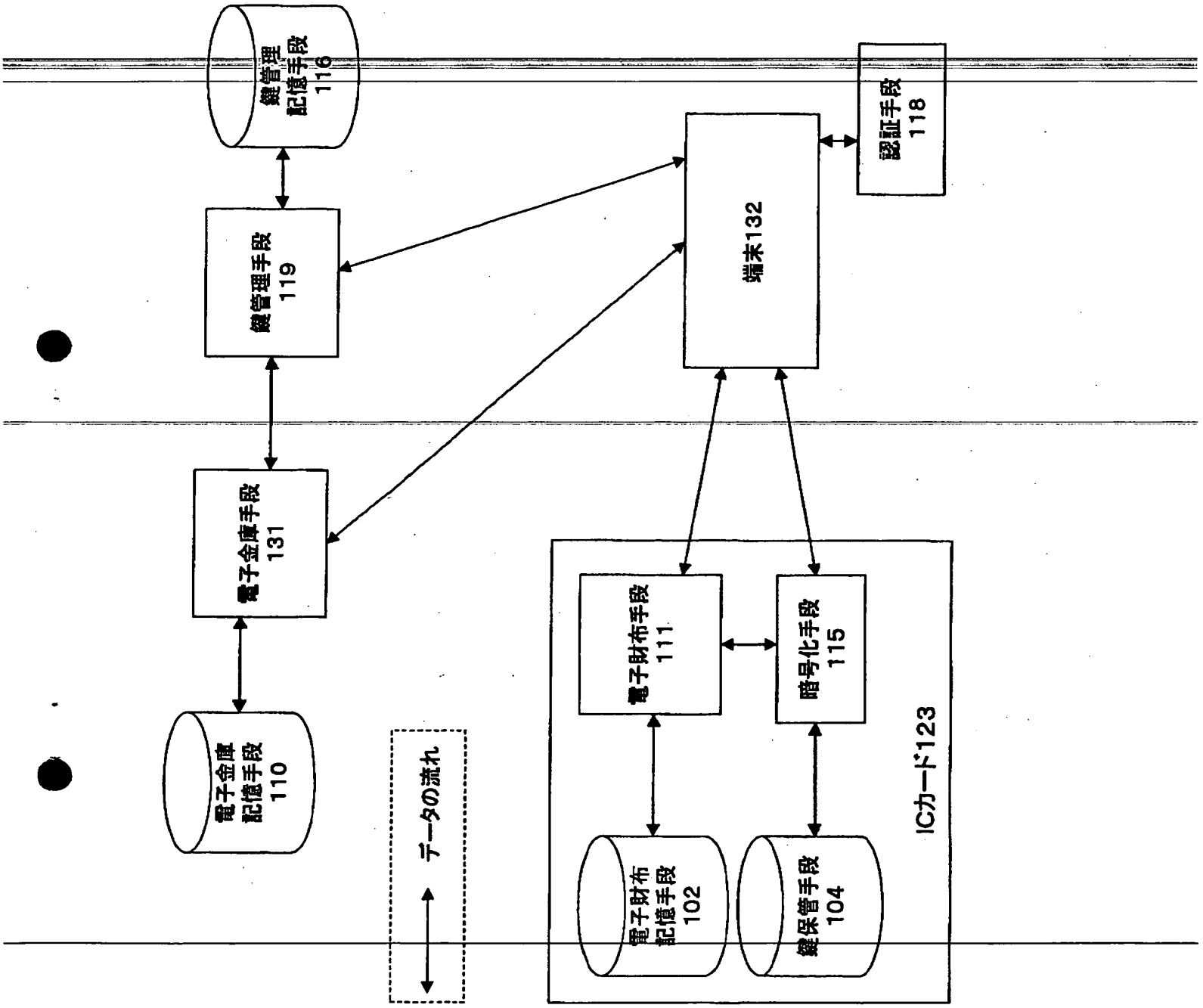
【図９】


鍵管理記憶手段116
インデックスファイル853
X
A
B
ファイル803
鍵情報491
ファイル804
認証情報891
X…認証情報のハッシュ値
A…ファイル803のパス情報
B…ファイル804のパス情報

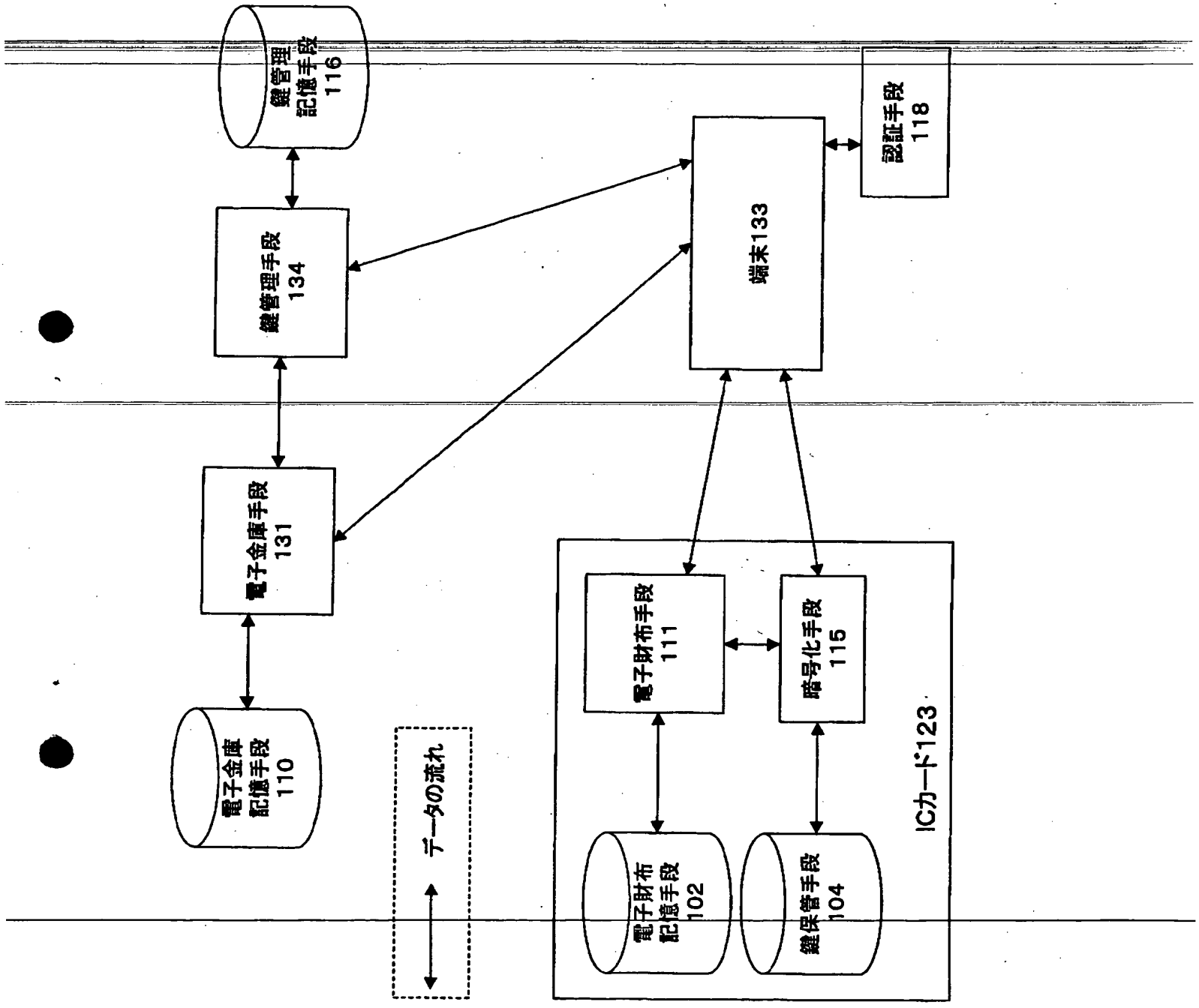
【図１０】


鍵管理手段
106
認証手段
118
端末117
鍵管理
記憶手段
116
電子金庫手段
113
電子財布手段
111
暗号化手段
115
電子金庫
記憶手段
110
データの流れ
ICカード123
電子財布
記憶手段
102
鍵保管手段
104

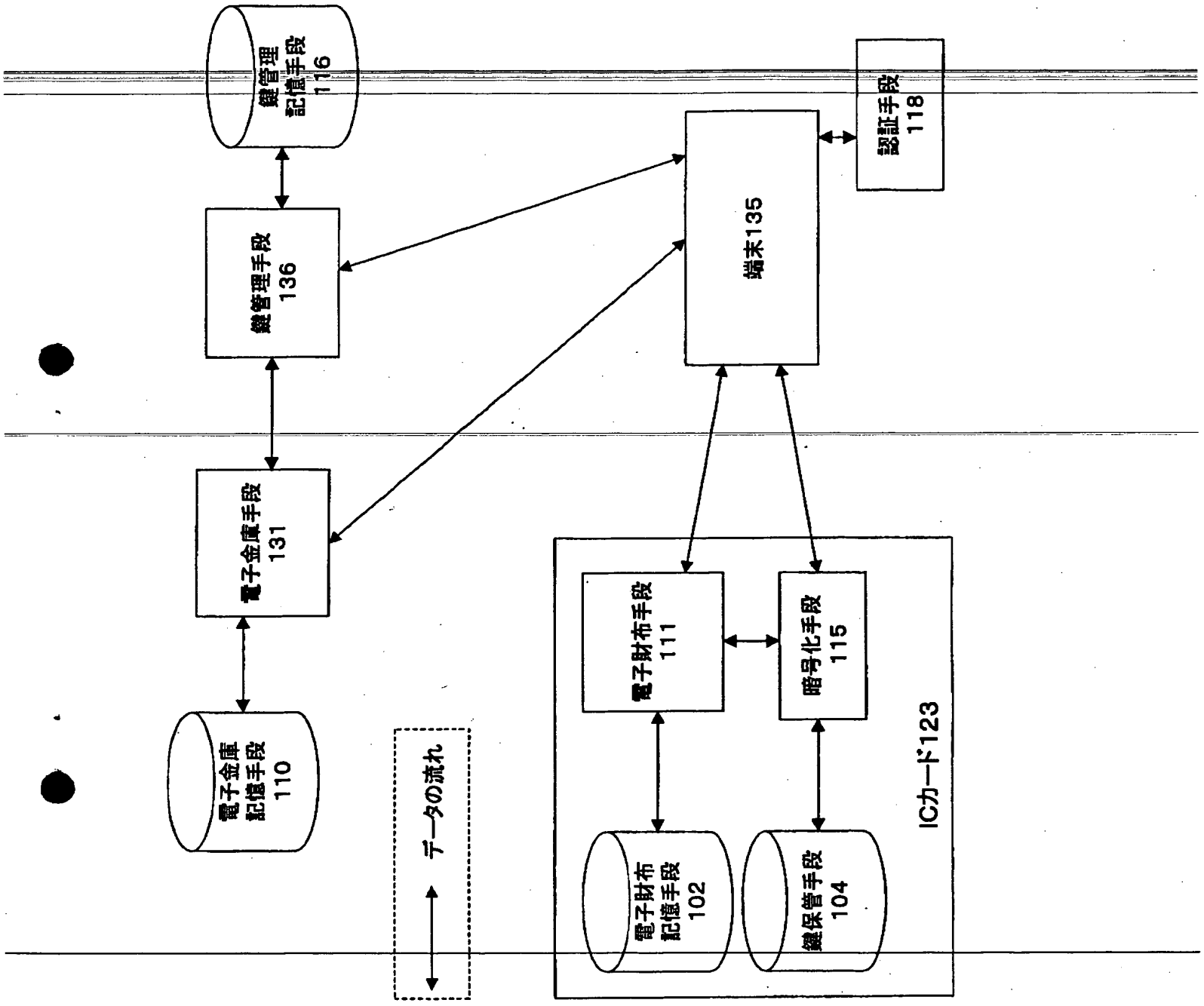
【図１１】


鍵管理
記憶手段
116
認証手段
118
鍵管理手段
119
端末132
電子金庫手段
131
電子財布手段
111
暗号化手段
115
電子金庫
記憶手段
110
データの流れ
ICカード123
電子財布
記憶手段
102
鍵保管手段
104

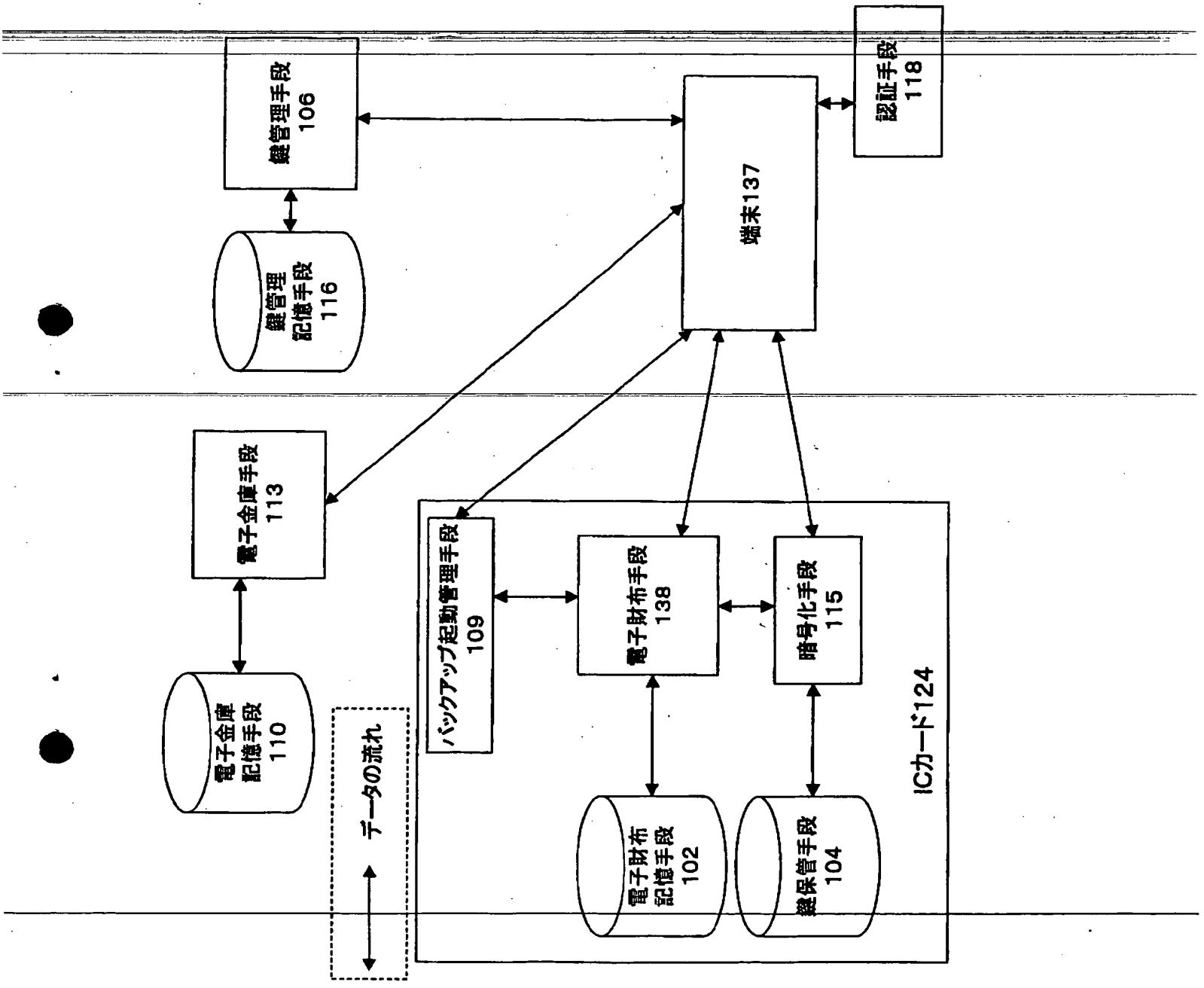
【図１２】


鍵管理
記憶手段
116
認証手段
118
鍵管理手段
134
端末133
電子金庫手段
131
電子財布手段
111
暗号化手段
115
電子金庫
記憶手段
110
データの流れ
ICカード123
電子財布
記憶手段
102
鍵保管手段
104

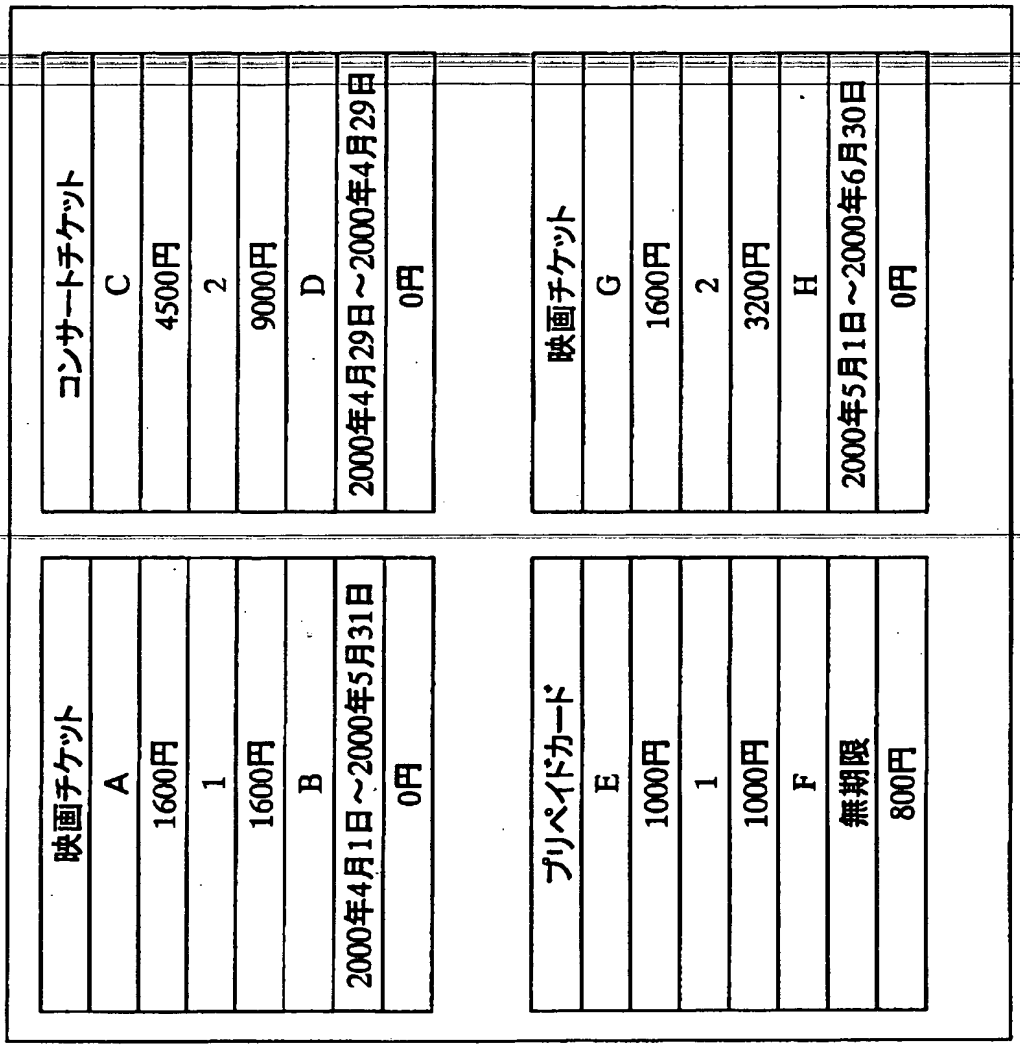
【図１３】


鍵管理
記憶手段
116
認証手段
118
鍵管理手段
136
端末135
電子金庫手段
131
電子財布手段
111
暗号化手段
115
電子金庫
記憶手段
110
データの流れ
電子財布
記憶手段
102
鍵保管手段
104
ICカード123

【図１４】


鍵管理手段
106
認証手段
118
端末137
鍵管理
記憶手段
116
電子金庫手段
113
バックアップ起動管理手段
109
電子財布手段
138
暗号化手段
115
電子金庫
記憶手段
110
データの流れ
ICカード124
電子財布
記憶手段
102
鍵保管手段
104

【図１５】



出証特２０００－３０６８１６２

【図１６】

映画チケット
A
1600円
1
1600円
B
2000年4月1日～2000年5月31日
0円

映画チケット
G
1600円
2
3200円
H
2000年5月1日～2000年6月30日
0円

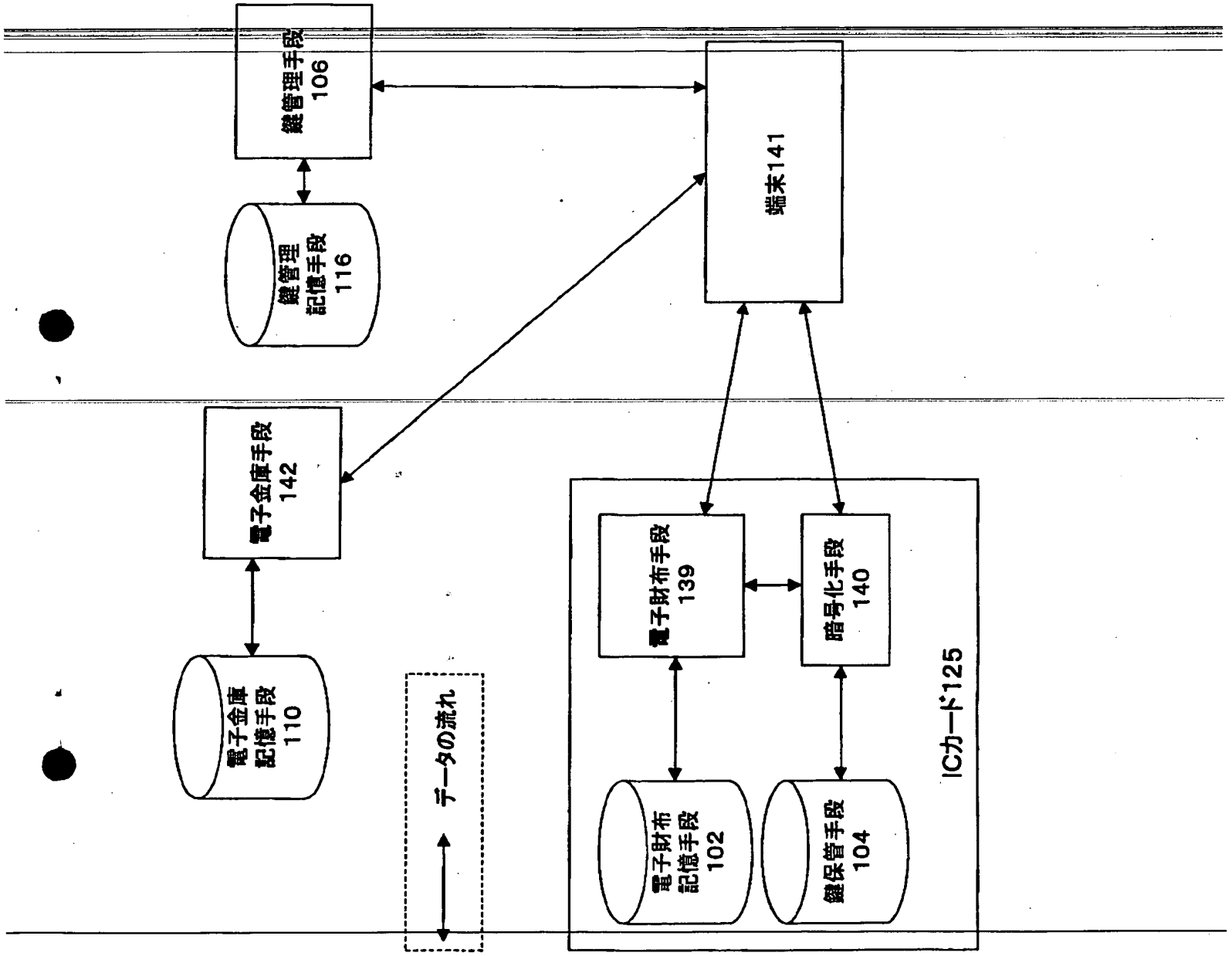
(a)

プリペイドカード
E
1000円
1
1000円
F
無期限
800円

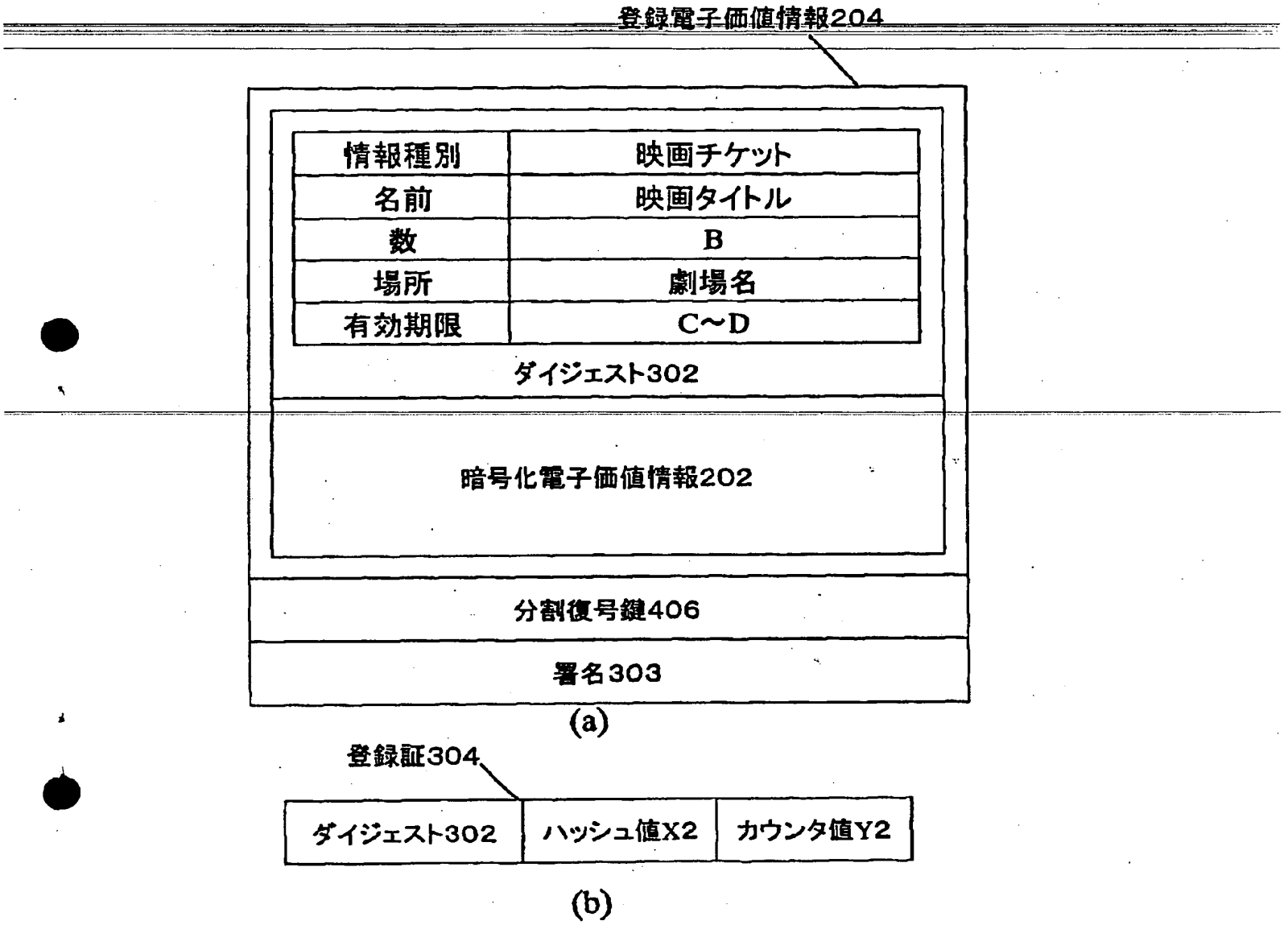
映画チケット
G
1600円
2
3200円
H
2000年5月1日～2000年6月30日
0円

(b)

【図１７】


鍵管理手段
106
鍵管理
記憶手段
116
端末141
電子金庫手段
142
電子金庫
記憶手段
110
データの流れ
電子財布手段
139
暗号化手段
140
ICカード125
電子財布
記憶手段
102
鍵保管手段
104

【図１８】


登録電子価値情報204
情報種別
映画チケット
名前
映画タイトル
数
B
場所
劇場名
有効期限
C～D
ダイジェスト302
暗号化電子価値情報202
分割復号鍵406
署名303
(a)
登録証304
ダイジェスト302
ハッシュ値X2
カウンタ値Y2
(b)

【書類名】　要約書

【要約】

【課題】　ローカルに存在する電子価値情報の安全性を確保するためのバックアップ手段を提供すること。

【解決手段】　電子財布手段１０１は電子財布記憶手段１０２上の電子価値情報を端末１００を介して電子金庫手段１０３に送り、電子金庫手段１０３は電子価値情報に対する登録証を生成し、電子金庫記憶手段１１０上に前記電子価値情報と前記登録証を組として保管し、前記登録証を端末１００を介して電子財布手段１０１に返し、電子財布手段１０１は前記登録証を電子財布記憶手段上に保管する。電子財布手段１０１は前記登録証を端末１００を介して電子金庫手段１０３に提示することことによって、前記登録証に対応する電子価値情報を取得することが可能であり、これによって電子価値情報のバックアップと復元を実現され、電子価値情報の安全性が得られる。

【選択図】　図１

出証特２０００－３０６８１６２